Online and technology-facilitated trafficking in human beings

Full report

G R E T A
Group of Experts
on Action against
Trafficking
in Human Beings

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Online and technology-facilitated trafficking in human beings

Full report

Report prepared by
Dr Paolo Campana
Associate Professor, University of Cambridge
United Kingdom

April 2022

Council of Europe

French edition:
La traite des êtres humains en ligne et facilitée par les technologies

All other correspondence concerning this document should be addressed to the Secretariat of the Council of Europe Convention on Action against Trafficking in Human Beings
trafficking@coe.int

All photos: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Printed at the Council of Europe

Table of contents

Abbreviations used in the text

AI:	Artificial Intelligence
ASW:	Adult Service Website
CoE:	Council of Europe
CID:	Criminal Investigation Department
CSE:	Child Sexual Exploitation
CV:	Curriculum Vitae
EAW:	European Arrest Warrant
EIO:	European Investigation Order
EJN:	European Judicial Network
EU:	European Union
GDP:	Gross Domestic Product
GDPR:	General Data Protection Regulation
GRETA:	Council of Europe's Group of Experts on Action against Trafficking in Human Beings
HDD:	Hard Disk Drive
JIT:	Joint Investigation Team
ICT:	Information and Communication Technology
ISP:	Internet Service Provider
MLA:	Mutual Legal Assistance
NGO:	Non-governmental Organisation
OSINT:	Open Source Intelligence
THB:	Trafficking in Human Beings
TOR:	The Onion Router
VOIP:	Voice over Internet Protocol

Introduction

Internet, and information communication technology (ICT) more generally, play a major role in shaping our lives. The Covid-19 pandemic has laid bare the extent to which the Internet and ICTs are now integral to a variety of activities and social interactions – and it has accelerated their relevance. The criminal landscape is no exception – and this extends to trafficking in human beings (THB).

There is little doubt that technology poses challenges – as well as opportunities – to law enforcement and NGOs alike. At the same time, the evidence base on online and technology-facilitated THB remains limited and patchy. At the moment, the best evidence available comes from a rather small set of studies, typically based on a small number of interviews with police officers and NGO personnel – often carried out in a very limited number of countries – as well as from a handful of reports from international organisations. This study moves beyond anecdotal evidence by offering an analysis of online and technology-facilitated THB based on evidence *systematically* collected from State Parties to the Council of Europe (CoE) Convention on Action against Trafficking in Human Beings. Such evidence has been supplemented with information from NGOs providing assistance to THB victims as well as tech companies.

The scope of the present study is rather broad. It offers an assessment of the extent to which technology impacts THB as well as an exploration of the traffickers' *modus operandi* in the context of online and technology-facilitated THB. At the core of this study is an exploration of the operational and legal challenges that State Parties – and to some extent NGOs – face in detecting, investigating and prosecuting online and ICT-facilitated THB, as well as identifying victims and raising awareness among at-risk groups. Crucially, the study also explores the strategies, tools and 'good practices' adopted by State Parties and NGOs to overcome such challenges and enhance their response to online and technology-facilitated THB. This work teases out similarities across countries as well as country-specific experiences. Particular emphasis is placed on training – as investments in human capital are as important as those in technical tools.

This study has been conducted as part of a long-standing interest of the Council of Europe in the issue of technology and human trafficking. Besides offering a *systematic assessment of the current evidence base*, this study also seeks to provide the Council of Europe Group of Experts of Action against Trafficking in Human Beings (GRETA) and other entities with a tool to carry out future assessments and track changes in both the technological and behavioural landscapes.

Methodology

The evidence from this study was collected through a novel questionnaire that included both open-ended and closed-ended questions. The questionnaire was produced in three versions (presented in the Annexes): a longer version for State Parties (40 questions) and two shorter versions for NGOs (14 questions) and tech companies (11 questions). The design of the questionnaire has been informed by a landscape analysis carried out in October – December 2020 covering a variety of sources: international organisations, academia, NGOs as well as the private sector (see Annex A for details). The questionnaire was built in consultation with GRETA Members and the Council of Europe Secretariat in January – March 2021. Responses were received from 40 State Parties[1], 12 NGOs[2] and 2 tech companies[3] in June – July 2021 (one late response reached the Council of Europe Secretariat in September 2021). Analyses were then carried out in June – September 2021. This is a rather tight timeframe for a study covering a fairly vast range of issues, countries and entities. While this study offers a detailed assessment of a large evidence base, it is by no means exhaustive nor without limitations. These are discussed in the remainder of the text whenever relevant.

This study follows Latonero (2012: 9-10) in defining technology as "information and communication technologies, particularly those constituting digital and networked environments. Technologies that allow users to exchange digital information over networks include the Internet, online social networks, and mobile phones".

Technology is here to stay – and with it, structural changes in the way offenders operate, opportunities open up and existing vulnerabilities are exacerbated. There is thus a need for State Parties to adapt and equip their law enforcement agencies and criminal justice system with capabilities in step with this (constantly) changing environment. This study offers some evidence-based recommendations to this end.

[1] Albania; Armenia; Austria; Azerbaijan; Bosnia and Herzegovina; Belarus; Belgium; Bulgaria; Croatia; Cyprus; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Latvia; Lithuania; Luxembourg; Malta; Republic of Moldova; Monaco; Montenegro; Netherlands; North Macedonia; Norway; Poland; Portugal; Romania; San Marino; Slovakia; Slovenia; Spain; Sweden; Switzerland; Ukraine and United Kingdom.

[2] 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 and IBM.

Summary of the report

The impact of technology on trafficking in human beings

The impact of technology on trafficking of human beings is of particular concern during two stages of the trafficking process: **recruitment** and **exploitation**. Evidence submitted by State Parties points to an "increasing" relevance of technology in the context of THB, with the majority of State Parties now considering the impact of technology on THB to be either "very important" or "important".

State Parties have noted the increasing relevance of online materials, advertisements, and sites/applications (or 'apps') in the search for jobs as well as the increasing relevance of online socialisation and personal interactions. In turn, both create opportunities for THB offenders and exacerbate existing vulnerabilities. Technology has changed the way people interact and this is reflected in the criminal landscape, including THB. This is a structural change that law enforcement and criminal justice systems need to adapt to.

Technology can play a role in the **recruitment** stage by facilitating the identification, location and contact of potential victims. Different mechanisms are at play depending on the type of exploitation.

In the context of recruitment for **sexual exploitation**, several State Parties have identified cases of job advertisements linked to THB and uncovered evidence of recruitment via social media platforms as well as dating applications. A common strategy is the so-called **"lover boy" technique**: a type of online recruitment in which a trafficker identifies and contacts a potential victim via an online platform, gets to know their hobbies and interests as well as their personal and family situations. The trafficker then offers empathy and support to the

potential victim in the context of a romantic relationship – seeking to gain trust and subsequently establish control over the victim.

There is ample evidence from several countries of cases of victims' **blackmailing**. This is often done by first collecting "compromising" information about the victims—for instance, by asking for naked pictures or videos—and then using the information to coerce them into prostitution.

During the **exploitation stage**, technology can facilitate the **sale** of sexual services provided by THB victims. There is ample evidence from several countries of Internet websites used to advertise sexual services. Among such advertisements, there are services provided by THB victims. Moreover, while live-streaming is often connected to child sexual abuse, a handful of countries have suggested that such live streaming might also involve adult victims of THB.

Further, technology can be used to **coordinate activities**. Crucially, technology allows for a **separation** between the place where the sexual activity is performed and the place where coordination takes place. This has important implications for law enforcement.

Countries have provided evidence of technological tools used by traffickers to **monitor and control** victims during the exploitation stage. Blackmail and the use of compromising information against victims can also be used to exert control during this stage.

Emerging trends in the context of sexual exploitation noted by various countries include the expansion of "live web cams" and "pay-as-you-go" video chat applications and increasing use of apps to control victims. Such web cams and video chat applications can be used to live stream sexual acts performed by THB victims. A few countries have noted that the Covid-19 pandemic has increased the opportunities for traffickers to establish online contacts with vulnerable individuals.

In the context of trafficking for **labour exploitation**, evidence provided by State Parties indicates that ICTs are mainly employed to **recruit** victims, particularly through **online job advertisements.** Such advertisements are not only published on classified job websites, but also posted and circulated on social media in specialised job searching groups and mutual aid groups. Several countries have highlighted the relevance of webpages meant to foster information exchange among migrant workers as a recruiting space targeted by traffickers.

An emerging trend in the context of labour exploitation, reported by some countries, includes a rise in cases of recruitment through the Internet and social networks. This is believed to have been accelerated by the outbreak of Covid-19. While technology does not seem to play a noticeable role in the exploitation stage, countries have flagged up the increase of opportunities to exploit THB victims offered by the 'gig-economy', particularly delivery platforms.

There is no evidence of any relevant role played by the **Dark Web** in the context of adult THB (the circulation of child sexual exploitation materials is outside the scope of this study). Similarly, **cryptocurrencies** appear not to be widely used in the context of THB (on the contrary, they are used to purchase live streaming of child sexual abuses).

Evidence submitted by **NGOs** paints a similar picture. They have identified the use of Internet and social media in all stages of human trafficking, and particularly in relation to (a) recruitment; (b) exploitation; and (c) exertion of control and pressure over victims. In

addition, traffickers can use ICTs, including social media and encrypted apps, to continue contact with THB victims after they have left the exploitative situation, often to prevent them from filing complaints and seeking justice.

Emerging trends based on evidence from NGOs suggest an increase in the exploitation of children via **webcam and social media**. There have been suggestions that offenders have started to use **online games** to approach potential victims.

Finally, the available evidence base suggests that the use of technology complements rather than substitutes personal, offline interactions. Technology and in-person interactions are best seen as integrated.

Challenges in detecting, investigating and prosecuting technology-facilitated THB

Challenges to detection

Detecting instances of online and technology-facilitated human trafficking and identifying victims remains very challenging. State Parties have highlighted a number of challenges:

- The constantly-growing volume of online activities/interactions. Policing the Internet is very resource intensive and subject to legal restrictions (including privacy laws and limitations to the use of web crawlers in some countries);
- The volume of online advertisements (open and classified) for both sexual and non-sexual services is often too vast to be manually searched;
- Difficulties in identifying both perpetrators and victims as they may use nicknames and aliases when operating online and may use anonymising software (e.g., VPNs);
- Use of encrypted communication between traffickers and victims. Conversations between traffickers and victims take place in closed groups;
- Fast-changing behaviour of Internet users;
- Challenges in sorting online advertisements to identify those related to THB both in the context of sexual and non-sexual services. Red flags in relation to advertisements related to both sexual and labour exploitation are still underdeveloped or not consistently utilised;
- Absence of specialised units within the police and/or lack of specialised THB investigators with advanced computer skills. Lack of officers trained to carry out covert operations on the Internet. Cyber-operations can be lengthy and time-consuming;
- Time-consuming process of sending requests to social media companies and lack of response from some of them;
- Short data retention periods for IP addresses and difficulties in accessing them.

Challenges to investigations

Data encryption is seen as the most severe challenge faced by State Parties (severity score of 80 out of 100). This is followed by the large volume of data (71), speed of technological change (66), lack of technical equipment (63), inadequate legislative tools (61), lack of technical knowledge among law enforcement (53) and lack of assistance from the private sector (46).

Data encryption protocols included in popular apps and online services are widely seen as problematic. Encryption also restricts the possibility to monitor communications. A few countries have hinted at the existence of tools to decrypt some types of devices. However, this is a constantly evolving landscape that requires (large) investments in both training and software. Steps taken to overcome this issue include the establishment of cybercrime units/centres tasked with working on decryption technology. Further, there is value in pooling resources at the supranational level in the development of technological products, such as decryption software and web-crawlers.

Electronic communications and ICT devices generate a **large and constantly growing volume of data** which, in turn, poses substantial strain on investigators. This strain impacts investigators' ability to extract and carefully scrutinise the data, which itself requires specialised pieces of software as well as specific training on how to systematise and search within such large bodies of evidence.

There is a broad consensus that building capacity in handling large amount of **electronic evidence** is crucial. However, such capacity needs to be constantly updated. Countries have noted that challenges are posed not just by the growing amount of data generated by online platforms and social media, but also by the changing **behavioural patterns** of their users.

Lack of technical equipment has been flagged as a challenge by several countries. Specialised software and hardware can come with hefty price tags and often require constant updates and expensive licensing agreements to keep up with the speed of technological change. The **need to keep up with technological change** can have a considerable impact on police budgets. This is an issue that has been raised by several countries regardless of their level of GDP (gross domestic product).

Investments in human capital are as important as those in software and hardware, if not more, particularly as they relate to the **lack of, and need to develop technical knowledge among law enforcement**. Evidence has pointed to a need to develop knowledge on (a) the emergence of new trends and changes in the use of technology; (b) the emergence of new apps and services in a tech market that is characterised by a rapid change and (c) the development of new security protocols and encryption methods. Crucially, knowledge needs to be distributed cleverly within an organisation. For instance, the lack of specialist officers at the local level can create **bottlenecks in the investigations**, if assistance from a (busy) centralised unit needs to be repeatedly sought.

Several countries have highlighted the need to **provide additional technical training to all police officers**, including knowledge on technology and how it works. Similarly, adequate training on the acquisition and handling of **electronic evidence** needs to be provided to the largest number of relevant officers and should be made a regular topic in training curricula

for police officers. In more complex cases, teams with multidisciplinary skill sets might need to be set up (e.g., by bringing together investigators, financial specialists and cybercrime specialists).

Further challenges include issues stemming from the inadequate **data retention obligations** imposed on Internet Service Providers (ISPs), and the application of privacy laws, for example in relation to web-crawlers.

Challenges to prosecution

Overall, the challenges to prosecution score lower than those to investigations, with only "obtaining evidence from other countries" scoring slightly higher than 50 (out of 100). This is followed by lack of training among prosecutors (40); inadequate legislative tools (38) and assistance from the private sector (33). Extradition of suspects (28) and attribution of jurisdiction (16) appear to play a marginal role.

Adequate **training of prosecutors** is seen as key to ensuring that ICT-facilitated cases are robust, that electronic evidence is properly collected and utilised, and that cases are adequately presented to a judge/jury. Some State Parties have noted instances in which prosecutors were not familiar with procedures to request electronic data from private companies or with those to obtain evidence and cooperation from other countries (e.g., via a Joint Investigation Team, JIT, or a European Investigation Order, EIO).

Some State Parties have raised the issue of dealing with electronic material, particularly in the context of **GDPR obligations** (EU General Data Protection Regulation). Concerns were also raised around international data protection regulations that can hinder the gathering, storing, and processing of information obtained with technological investigative techniques (such as web crawling).

Challenges have been noted around IP addresses and electronic evidence. IP addresses need to be linked to screen names and users where possible. However, screen names can be changed at any time and are often used by suspects interchangeably.

A further challenge relates to the **presentation of evidence** in front of a jury (and judge), as technical evidence in ICT-facilitated cases can be complex and often needs to be presented by an expert. Developing in-house expertise among officers on how to effectively and accurately present electronic evidence may be increasingly valuable.

Challenges to international cooperation

The lengthy turnaround time for the processing of **Mutual Legal Assistance requests** (MLAs) has been indicated by the vast majority of State Parties as one of the major obstacles to international cooperation. Mutual legal assistance procedures are seen as slow, sometimes unpredictable and in need of internationally agreed templates. This issue is particularly exacerbated when cooperation takes place outside the EU legal framework.

Cooperation outside the EU legal framework is seen as a time-consuming process and is characterised by greater intricacies due to the lack of harmonisation among different legal systems, alongside elements of unpredictability and inconsistency. Clearer operating procedures, enhanced regular exchange among contact points, clearly setting out MLAs' requirements, and discussion at the outset would help smoothen the process.

Technology allows criminal networks to organise and control exploitation activities from afar – for example, from another country – often knowing that requests for judicial cooperation will not be fulfilled in a timely manner, if at all. This creates the need for enhancing, or in some cases setting up, agreements with the victims' countries of origin if they are outside the EU.

Challenges in processing MLAs can also result from the **lack of adequately trained personnel** to compile and handle requests as well as the use of outdated technology.

Electronic evidence can make it difficult to identify the exact location of the data and the country under whose jurisdiction such data fall, thus making the drafting of an MLA request challenging.

Calls have been made for a common legal framework for the **rapid exchange of digital evidence**. Several countries have expressed concerns about the lack of a homogeneous regulation of **data retention**, hindering the exchange of electronic evidence. Overall, State Parties have expressed the need for a more comprehensive framework regulating the retention and transfer of electronic evidence and a common legal framework to replace current ad-hoc bilateral working agreements between States and private companies holding the data (see also below). State Parties have also highlighted the need to improve the exchange of data during investigations.

Challenges to cooperation with private companies

Several countries have indicated that ISPs (Internet service providers), content hosts and social media companies have generally been cooperative when it comes to issues related to THB and child sexual exploitation. Nonetheless, a number of challenges have been identified. These include:

- **Obtaining a timely response** from some ISP companies and content hosts. Approaching hosts via rogatory letters sent through relevant authorities might entail long waiting periods with the risk of content being deleted by the time the request is acted upon;
- **Clarifying the legal requirements** under which ICT companies and providers of Internet services operate. Some countries have expressed concern that some ISPs impose formalistic, "legally unjustified" requirements on law enforcement agencies and do not adequately motivate and explain refusals;
- **Lack of a designated contact point** within private companies. Large companies operating in multiple countries often lack staff possessing the language and legal skills relevant to each country they operate in;

- **Lack of knowledge** among content hosts and social media companies on which national agency is responsible for which decisions, e.g. taking down illegal content. There have been suggestions to introduce the role of 'trusted flagger', i.e. identify specific agencies that are tasked with liaising with international providers to take down content. The trusted flagger would have an open communication channel with the companies and build mutual trust.

Evidence from NGOs

Broadly speaking, the evidence from NGOs points to similar issues to those discussed above. More specifically, NGOs have highlighted the following issues:

- **Lack of capacity** among law enforcement, which includes lack of training, hardware and software and limited use of special investigation techniques. There is also a lack of specialisation among some police forces and judiciary related to technology-related THB;
- **Fast-changing technological landscape and offenders' *modus operandi***. Professionals can find it hard to keep up to date with technology-facilitated THB, hindering their ability to promptly identify cases. Knowledge about technical landscape and practices (*modus operandi*) often sits in silos;
- Use of private forums, chat rooms or encrypted apps for contacts between offenders and victims. This makes it difficult to (a) detect such contacts and (b) acquire them as evidence to be used in court. NGOs have suggested including in chat rooms and apps information/warnings on the safe use of private channels of communications;
- **Rules about data protection and privacy** can hinder the identification of victims as well as traffickers. GDPR rules limit the use of technology to detect digital trails left by both victims and offenders;
- **Lack of interdisciplinary technology collaboration** among private companies, public agencies and NGOs to fully exploit the increasing amount of data on THB;
- **Lack of a technology strategy** in national action plans for combatting THB;
- **Lack of capacity, resources and technical tools** among NGOs to detect technology-facilitated online exploitation on a regular basis;
- **Conflicting goals** or different approaches between NGOs and law enforcement.

Evidence from tech companies

As noted above, only two companies provided replies to the questionnaire. Facebook noted that content related to human trafficking is "rarely reported" by users. IBM noted several obstacles to cooperation with law enforcement, including concerns about the legality of such cooperation, especially relating to data privacy and the legal complexity of multiple jurisdictions. IBM also called for clarifications on the international legal permissions for gathering and sharing data with law enforcement.

Strategies and good practices

Detection of ICT-facilitated cases of THB

Countries have indicated pursuing a variety of strategies to detect online and ICT-facilitated cases of THB. A widely cited strategy is **Internet monitoring,** including forums and, in some cases, TOR networks (Dark Web). This is combined with the use of **Open-Source Intelligence (OSINT),** meaning collecting data from social media and other publicly available online sources about a person's network of contacts, living conditions and financial situation.

Some countries have formed **"cyber-patrols" with specialised officers** tasked with carrying out OSINT investigations on the Internet. Some jurisdictions allow for covert online investigations (cyber-infiltration).

Web-scraping tools specifically developed for extracting information from websites are used by some law enforcement agencies, particularly to identify risk and vulnerability on Adult Services Websites (ASWs).

Linked to OSINT investigations, there is the utilisation of **social network analysis techniques** to understand and reconstruct the network of contacts of an offender and/or victim. **Relational information** is key: information collected from different sources can be systematised and used **to reconstruct criminal networks,** i.e. relations among places, offenders and victims**.**

Not all State Parties, however, have indicated using "proactive" strategies. A few State Parties have indicated that their investigations into ICT-facilitated THB remain "reactive".

Several countries have implemented **systems for Internet users to report content and websites** that they suspect are linked to illegal activities, including sexual and labour

exploitation. In some countries, for example, France, Internet access providers and website hosts are required to assist law enforcement in combatting the dissemination of materials related to specific offences, including THB. They are required to set up an easily accessible and visible system enabling any person to flag up suspicious material.

Some countries have reported the use of **awareness-raising campaigns** to increase detection of ICT-facilitated THB cases. These include awareness campaigns for clients who use websites hosting advertisements for sexual services to inform them of the risk of coming across THB cases (Belgium and UK) and campaigns providing information on how to look for safe work opportunities (Poland and Bulgaria). The authorities of some countries have leveraged on social media to disseminate targeted information, sometimes by creating targeted Facebook advertisements linked to a tip-off line.

Investigation into ICT-facilitated THB cases

In some countries, law enforcement agencies carry out **cyber-infiltration** of criminal networks by using covert techniques as well as undercover investigations. Several countries have expressed the need to increase such **undercover investigations**, hence investing in the training of specialised officers. There is wide consensus on the importance of acquiring and having access to **specialized software** as well as on the importance of big data and improving big data capabilities. The development of tools for downloading information from mobile phones bypassing a passcode and for decrypting conversations over communication apps is also seen as key.

Investing in human capital is widely seen to be as crucial as investing in technological equipment. Investing in human capital may mean providing law enforcement officers with continuous training and development activities based on local and global best practices. Likewise, several countries have noted the importance of including specialised investigative officers with 'digital knowledge' in the THB investigations. One model would see the presence of personnel specifically trained in conducting investigations on the Internet and social networks embedded within each unit specialised in the fight against THB. This would create **technical support groups** for investigators. Such groups could be staffed by sworn police officers or non-sworn police officers. This idea **moves away from the traditional police model** based uniquely on sworn police officers and adopts the principles – already followed by some police forces – of having non-sworn officers in more technical roles (e.g., analysts).

Further, State Parties have highlighted the value of **inter-agency investigative work** with the involvement and cooperation of a wide range of specialised agencies – as well as knowledge sharing across institutions. Similarly, countries have noted the importance of **enhancing cross-border cooperation** through, for example, mutual exchange of officers with the countries of origin of victims. At the operational level, countries have noted that investigation could be facilitated by an **easier cross-national preservation of evidence and its access.**

When conducting investigations, it has been suggested that countries should not over-rely on a **prescriptive list of indicators**, e.g. to identify high risk online advertisement, but also rely on layering of information of different nature, including intelligence, open-source

information, and police records. The **importance of network analysis and relational data** has been stressed.

Albeit time-consuming, **strategic analysis** generating knowledge on emerging trends and up-to-date information on offenders' *modus operandi* (including technology and websites used by offenders) is seen as very valuable.

Technology can also be used to **facilitate the collection of evidence from victims** both during the investigation and prosecution of THB cases and to lessen the burden on victims.

Fostering international cooperation

State Parties have identified the following good principles to foster international cooperation:

- Leveraging on resources available within agencies such as Europol and Eurojust, and setting up JITs, for those countries who are part to the EU Judicial Framework;
- Establishing contact with other interested parties at the early stage of an investigation;
- Developing a very good understanding of the legal context and opportunities for cooperation with other countries;
- Creating coordination meetings to exchange information and evidence as swiftly and as quickly as possible and to lay out a common strategy from the *outset*;
- Developing a common understanding of standardised approaches and ensuring transnational interoperability of law enforcement agencies through transnational training sessions.

Cooperation among non-police authorities, often neglected, can be as relevant as police cooperation, particularly in the context of THB for labour exploitation (e.g., between labour inspectorates).

Victims' identification and assistance

Facial recognition appears to be widely used in the case of Child Sexual Exploitation (CSE). However, its use appears to be more limited outside of CSE. A few countries have indicated the use of tech tools to identify victims of THB leveraging on big data (mostly web-crawlers but also facial recognition tools under stricter conditions).

Several countries rely on indicators for the identification of THB case ("**red flags**"); however, these are 'general' THB indicators and not specific to ICT-facilitated THB. While there is a clear need to develop indicators specific to ICT-facilitated THB, authorities have also cautioned against over-relying on "red-flags". Even in cases in which indicators have been developed specifically for the identification of victims on adult services websites (ASWs), as in the UK, the indicators show some clear limitations and are best used in conjunction with social **network analysis and human assessment** of the evidence.

Tech tools can be very valuable in performing data reduction and handling large volumes of information; however, they need to be employed by well-trained operators with knowledge of the specific topic/issue (e.g., THB). Using artificial intelligence and tech tools to identify victims

is not without issues, including ethical concerns and the potential for discrimination (e.g., profiling based on discriminatory criteria; see also below).

With regards to technology-based initiatives to assist victims and disseminate information to at-risk communities, countries have identified examples of (1) online self-reporting mechanisms and helplines, including digital assistance through a chat function; (2) online awareness-raising campaigns, often targeting specific at-risk groups (e.g., job seekers); (3) purposely developed apps and online tools; and (4) official materials made accessible online and translated in several languages. A good practice is working with private companies to produce **social advertising** (e.g., co-developed with and co-sponsored by social media). However, online campaigns should not replace direct, personal contacts with vulnerable individuals.

Evidence from NGOs

NGOs have stressed the importance of having **adequate and up-to-date information** that can be easily accessed online by trafficked persons and those vulnerable to exploitation and abuse. Such online platforms should also **allow for self-identification** of victims. This should be coupled with **awareness-raising campaigns**.

NGOs have further highlighted the importance of developing knowledge about ICT-related risks, and more generally technology-facilitated THB, also among organisations that assist victims, including counselling services. As **preservation of electronic evidence** is key to building strong investigations, it is crucial that counsellors and NGOs first respondents are familiar with strategies to preserve digital evidence (e.g., by storing chat histories).

Evidence from NGOs confirms that **"red flags"** for technology-facilitated THB cases are not widely used. NGOs report using standard indicators, but they call for a **review of such indicators** to consider the specificities of technology-facilitated ICT.

NGOs have identified examples of **tech-based initiatives** that they have developed to (a) foster online self-reporting; (b) establish contact with at-risk population, e.g., to break isolation and empower victims; (c) raise awareness among vulnerable and at-risk groups, and seek help, via purposely built apps and websites; and (d) produce online awareness campaigns.

Generally speaking, NGOs are increasingly making use of technology, but their overall level still remains "limited". There is a wide consensus that more can be done to leverage on technology, in particular with respect to the way technology is used to disseminate information; to approach potential victims and communicate with them; and to receive tips and reports.

NGOs have also raised some **critical issues** related to initiatives and tech tools, including the need for testing periods for new tools and—crucially—evidence on their effectiveness (which is still very limited). They called for **more evaluation and impact assessment** of the technology tools developed. Additionally, there is often no long-term financial strategy to promote and utilise the tools produced, including resources to keep them up-do-date. NGOs also stressed that, overall, there is still a limited availability of technological **tools that**

practitioners *can* use (to suits the needs of NGOs, tools need to be "cheap and 'easy to use'").

Further evidence from the landscape analysis

Other issues raised in the available evidence base include:

- The need to act upon information leveraged through technology (in a case discussed by Rende Taylor and Shih (2019), workers' reports via app-based feedback on exploitation in supply chains were found to be hardly acted upon);
- Technology should not be seen as a substitute for on-the-ground knowledge;
- Crowdsourcing the detection of victims might raise issues of privacy as well as the potential risk of vigilantism. While tips from customers are considered very valuable, crowdsourcing initiatives need to be closely scrutinised and balanced against the risk of creating virtual (and non-virtual) vigilante groups;
- The need to improve the collection and analysis of digital evidence to decrease the burden on victims (e.g., when asked to provide evidence against traffickers or in their defence).

Training: what is provided, what is needed

The vast majority of countries reported delivering training on THB. However, the levels and formats of training provided to **law enforcement** vary across countries. Some countries require all police officers that might come into contact with a potential victim to undergo such training while others limit training to specialised units.

There is a consensus on the fact that officers need to receive training on (a) how to detect THB cases and victims; (b) how to collect, store and process electronic evidence, including methods of extracting information from computers and other digital media; and (c) how to use relevant software, including **'Big Data Analysis'** and web-crawlers (where allowed by domestic legislation). **Training on OSINT** is seen as essential by several countries. Investigative techniques involving **covert online investigations** are also seen as increasingly important.

While most countries have reported providing elements of the abovementioned training, they have also flagged up issues, including (a) the need to keep training up to date and, in some cases, to considerably enhance current provisions; and (b) to increase the proportion of personnel that receives training. Some countries have expressed concerns about the limited training that is often provided in relation to ICT-related issues and, even more so, ICT-facilitated THB.

Looking ahead, the **risk of bottlenecks in the system** is particularly acute. As ICT-facilitated crimes, including THB, are likely to continuously increase, there is a need to not over-rely on centralised cybercrime centres. It is crucial to include general/basic **'cyber'**

knowledge in routine training provided to investigators rather than seeing this as a set of 'specialised' skills in order to avoid such bottlenecks.

Six broad areas emerge as critical for capacity building: collection and analysis of open source information (OSINT); data collection from social network profiles and communication apps as well as Darknet/TOR network; examination of information present on communication and information storage devices, including information deleted by users as well as knowledge on encryption; ability to corroborate data acquired from ICT sources with additional evidence acquired during the criminal investigation; identification of victims/potential victims in the online environment; economic and financial crime training with an element dedicated to online transactions and potentially cryptocurrencies.

Provision of **training to prosecutors and judges** in relation to ICT-facilitated THB is rather uneven across State Parties. Several countries have indicated that they are not currently providing any training on this phenomenon to the judiciary. Other countries provide general training on THB without any element specifically focused on ICT-related issues.

NGOs have expressed a need to receive training from domestic law enforcement authorities and international organisations on the latest developments in both the technological and THB landscapes, including changes in recruitment strategies. They also flagged up the need for training on international best practice and sharing of experiences across countries.

Legal instruments

Gaps in the current international framework

Overall, State Parties have expressed a positive view of the available legal instruments enabling cooperation across countries in combating THB. The CoE Conventions on Mutual Legal Assistance and on Cybercrime are considered among the "most commonly" used instruments and, overall, are judged as "adequate". Nonetheless, State Parties have identified some potential gaps and areas in which the current legislation might be improved. The main gaps identified relate to:

- Absence of a commonly agreed (standardised) legal environment underpinning exchange between Internet service providers and authorities when dealing with specific investigations;
- Provisions that allow for a more timely response from private companies to data requests;
- Provisions to compel private companies to disclose information upon direct request/order from another State Party;
- Provisions implementing shared rules on data retention;
- Provisions to facilitate the collection of victims' testimonies and their use in a different country;
- Issues around transnational measures against websites hosting materials that can be linked to the facilitation of victims' exploitation;
- Provisions introducing a "duty of vigilance" by companies on their entire supply chain;
- Use of terminology that does not always allow for legislation to evolve in parallel with changes in traffickers' *modus operandi*;
- Differences in the transposition of the THB offence (as per the UN Palermo Protocol) in domestic legislations.

The Cybercrime (Budapest) Convention and the fight against ICT-facilitated THB

The CoE's Cybercrime (Budapest) Convention is the most relevant instrument geared towards ICT-facilitated crime that is cited by State Parties.

State Parties consider the provisions related to **procedural law** as the most valuable in the context of ICT-facilitated THB (Chapter II, Section 2 of the Convention). Furthermore, they have highlighted the **importance of non-restricting procedural measures to offences explicitly listed** (e.g., those in Chapter II, Section 1) The Convention clearly achieves its full potential only when it is not restricted to the offences explicitly listed in Chapter II, Section 1. This is particularly true in the context of ICT-facilitated THB.

Several countries have indicated the utility of provisions included in Chapter III of the Convention on international cooperation as a legal basis for **gathering and sharing electronic evidence** across countries. The Convention establishes a network of contact points. While this is an important tool, looking forward, it is likely that – with the increasingly central role played by ICTs and the electronic evidence – such contact points will be under increasing pressure – and quickly overwhelmed if not adequately staffed. This speaks to the issue of **bottlenecks** within a system, where the contact point is located within the criminal justice system is key and can be very consequential.

Looking ahead, the following steps can allow the **Cybercrime Convention to be further utilised** to fight THB:

- Implementation of the Second Additional Protocol to the Convention, which was adopted in November 2021 and will be opened for signature on 12 May 2022;
- Completing the harmonisation of national legislations with the Cybercrime Convention to leverage on its full potential;
- Wider and enhanced training on the possibilities offered by the Cybercrime Convention as not all State Parties are currently using the tools available to their full potential;
- Greater awareness on the scope of the procedural provisions included in the Convention, as the evidence has suggested some degree of disagreement among respondent countries on the extent to which the current provisions can be applied to THB cases;
- Implementation of a procedure to accelerate provision of MLA by allowing for the possibility to send a request directly to an entity located in a foreign jurisdiction provided that the judicial authority of that country is notified;
- Building synergies between GRETA and the Cybercrime Convention Committee (TC-Y) to continuously assess the use of the Cybercrime Convention in the context of THB.

Challenges identified by NGOs

NGOs have noted "clear restrictions" related to **data protection (GDPR) and privacy rules**. Further, they call for legislation allowing for **digital forensics** as admissible evidence in all jurisdictions. Further challenges relate to updating regulations to take into account

cybercrime and the Internet as well as devising legislation and operating rules for digital investigations.

Domestic legal frameworks related to the removal of THB-related content

The great majority of countries have legal measures in place to regulate the identification, filtering, and removal of THB-related Internet content. The measures often do not specifically refer to THB but "illegal content" more generally (the exception being child sexual exploitation materials). In some countries, procedures to remove THB-related content require a court order. Some of these countries regard these procedures as "too rigid" or not effective, and they advocate for more efficient means. Finally, some countries have stressed that providers located abroad can easily bypass national legislations on the legal responsibility of host providers.

Human rights, ethics and data protection

Evidence from State Parties

All State Parties have indicated the adoption of domestic legislation regulating **data processing** and **data protection**. Regarding the **personal protection of victims**, a number of countries have noted the introduction of measures to prevent offenders from making contact with victims; the questioning of witnesses through videoconferencing to prevent contact with the defendants; and in some cases the possibility for victims to give evidence in court anonymously to protect their identity.

State Parties have indicated that they have **age-sensitive protocols** in place in the form of different sets of procedures and safeguards that are normally applied depending on whether the victim is a child (under 18). As for **gender-sensitive protocols**, all countries for which this information is available have indicated that they do not have such protocols in place, the only exception being Austria, which has indicated a separate support system based on the victim's gender.

Evidence from NGOs

As a standard procedure, NGOs ask for the victim's consent before sharing information with law enforcement. Issues arise when victims are reluctant to file a complaint with the police for a variety of reasons, including the risk of retaliation, social exclusion or potential for the victim's being deported. NGOs estimate that this is the case for "many trafficking victims". Issues of data protection and data sharing can generate **moral dilemmas**. While sharing data with law enforcement and filing complains *does* support investigations, which in turn can

potentially save and protect more victims down the line, it comes to a cost to the individual victim, which might be exposed to risks and threats.

NGOs have called for more attention to the **potential risks and harm generated by large scale data collection and tech tools**. They also called for further reflection and additional control measures on the use of data and their secured storage – and to ensure that data protection rules are followed.

Finally, there is very limited evidence of **gender-sensitive protocols** developed by NGOs. **Age-sensitive protocols** are normally in place based on whether the victim is a minor or an adult.

Further evidence from the landscape analysis

ICT can have a considerable impact on the **human rights** of individuals, including the rights to privacy, freedom of expression and freedom from discrimination. Technology-heavy policies to combat human trafficking need to be designed with consideration for human rights.

Key issues have been identified relating to **data privacy, ethics, transparency, accountability, and informed consent**. OCSE (2020) identified a number of ethical issues related to the development of technology to combat human trafficking, including: (a) protection of data privacy; (b) consent protocols signed by victims; (c) training for people handling sensitive data, particularly victims' data; (d) secure storage of data; (e) preventing the use of technology for obtaining sensitive data about vulnerable people (for instance, blanket collection of data over vulnerable or marginalised populations, creating risks of discriminatory practices); and (f) using technology in a way that does not infringe human rights of victims as well as those of the general population. ICAT (2019) and other sources have pointed to the sensitivity around data sharing. When data is shared between countries and/or relevant agencies, it needs to be done in accordance with the principles of privacy and confidentiality.

Gerry et al. (2016) warned about the risk of widespread **tracking tools** to combat human trafficking. While such technology can offer new opportunities to intervene in trafficking situations, it also consists of **a form of surveillance that is potentially highly invasive** on a person's privacy.

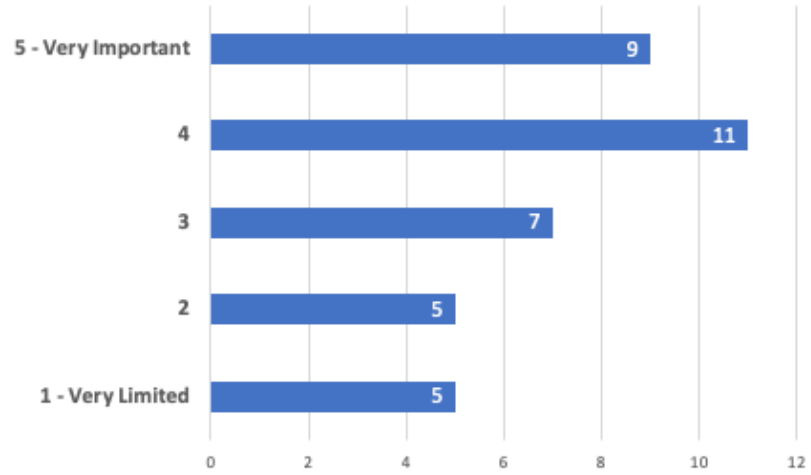
Finally few sources, including Milivojevic et al. (2020) and Gerry et al. (2016), have highlighted the importance of **not cutting victims out of technology**, as access to technology can be their only way to communicate with the external world, and may serve as an important coping mechanism. Removing access to technology can be disempowering to victims; promoting safe access to technology should be privileged instead. More generally, the best interest of the victim should be placed at the centre of any action.

1. The impact of technology on trafficking in human beings

1.1. Evidence from State Parties

The evidence submitted by State Parties confirms the increasing relevance of technology in the context of THB, and particularly in relation to recruitment and exploitation. Technology and online activities are becoming more and more relevant in people's lives – and this is mirrored in the context of THB. The majority of State Parties consider the impact of technology on THB to be either 'very important' or 'important' (Figure 1). [4]

Figure 1. Impact of technology on THB: State Parties



Note: N = 37

Among the countries that have reported a limited impact, some have also reported very limited or no cases of THB (i.e., low tech impact, low THB overall). For other countries, it is the usage of technology overall that is (still) rather limited (i.e., low tech usage, low tech impact). In this latter case, the picture might change as technology is embraced more widely. Indeed, some State Parties have pointed out the increasing relevance of online materials, advertisements and sites/apps in the search for jobs, as well as the **increasing relevance** of online socialisation and personal interactions. In turn, both **create opportunities** for THB offenders and **exacerbate existing vulnerabilities**.

1.1.1. Trafficking for sexual exploitation

In the context of **recruitment for sexual exploitation**, several State Parties have identified cases of job advertisements offering suspiciously high salaries, often in service sectors, which turned out to be a means to recruit individuals for exploitation. Several countries have pointed out the presence of highly deceptive or outright fake job advertisements, often published on widely-accessed websites and listed besides legitimate advertisements. Additionally, there is

[4] Three countries have not provided an answer to this question.

evidence of recruitment via social media platforms by individuals offering jobs, for instance, in hospitality (e.g., waitering) and agriculture. Offenders would normally make a promise of a (non-existent) well-paid job abroad, and then force the person to perform sexual services in the destination country.

According to the 2019 National Situation Report on THB compiled by the German authorities, 11% of victims identified were contacted or recruited through the Internet (N = 47). Of those 47 victims, 31 were contacted through a widely used social media platform and 13 through advertising portals (three victims were recruited using an 'other' Internet-based method). The Bulgarian National Commission for Combating Trafficking in Human Beings highlighted that potential victims contacted via social media platforms are "mainly young girls and women". The Dutch authorities reported that, based on the information present in the police system, social media platforms are used to recruit underage victims. According to evidence from Austria, recruitment tends to take place in the victims' country of origin.

When approaching potential victims on the Internet, offenders might adopt quite sophisticated *modus operandi*, often based on fake profiles showing high standard of living and considerable wealth. As reported by the Bulgarian authorities, "a number of investigations have found that before approaching their potential victims and starting the recruitment, perpetrators carefully examine the photos of their targets [in order to] explore their living conditions, social status and environment, family relations and relationship status, such as marriage, divorce or engagement. […] It is only after such careful examination that the perpetrators contact their victims, employing remarkable psychological skills of persuading and motivating victims to engage in certain behaviours". Evidence of such *modus operandi* is vast and comes from several countries, including Austria, Bosnia Herzegovina, Bulgaria, Belgium, Croatia, Hungary, Republic of Moldova, the Netherlands, Poland, Portugal, Slovakia, Sweden and Ukraine. Such *modus operandi* is often part of the so-called 'lover boy' technique, i.e. feigning a romantic relationship to coerce a victim into prostitution. As assessed by the Romanian authorities, among others, "the lover boy technique remains the most common tool". It consists in contacting a person via an online platform, getting to know their hobbies and interest, their family situation and personal circumstances (as well as vulnerabilities). Subsequently, the "trafficker approaches the victim with empathy, with a great willingness to help her and understand her, as well as to financially support her. Often, the victim is manipulated through promises of a serious relationship, sometimes with marriage requests, in the attempt of gaining her trust and then psychologically control her" (evidence from Romania). According to evidence from Belgium, victims recruited through social media platforms tend to show patterns of family instability, school dropout, low self-esteem and, more generally, psychosocial vulnerabilities.

Evidence from France suggests that THB networks of various nationalities, including South American, Eastern European as well as French nationals involved in the so-called trafficking '*de cité*' ('deprived neighbourhood pimping') use social networks to recruit victims. THB networks involving individuals from African countries appear to be the exception to this rule. A number of countries have provided evidence of recruitment carried out on dating applications (including the UK, Norway, Finland, Austria, Ukraine and Belarus).

There is ample evidence from several countries of cases of **blackmailing**. This is often done by first collecting "compromising" information about the victims, for instance by asking for

naked pictures or videos, and then use this evidence to coerce the person into prostitution. Offenders would first establish a relationship with the victim, gain their trust and then solicit "compromising" information. Evidence of such behaviour has been reported by several State Parties, including Bosnia and Herzegovina, Bulgaria, Croatia, the Netherlands, Finland, Lithuania and Sweden.

Some countries have provided examples of victims recruited online among individuals willing to provide sexual services; however, once recruited, they are then subject to exploitative working hours and very poor accommodation conditions, and faced with earning opportunities drastically different to those advertised (evidence from Hungary and Poland). Evidence from Poland also points to cases of women advertising sexual services who are targeted by traffickers, intimidated and forced to share their profits (a mechanism similar to extortion).

There is ample evidence from several countries of Internet websites used to **advertise sexual services**. Nested within such advertisements, there are also advertisements linked to services provided by THB victims. As noted by the British authorities, Adult Services Websites (ASWs) "continue to be the most significant **enabler of sexual exploitation** linked to human trafficking in the UK". ASWs are "attractive to offenders because they can require little user verification and provide access to a large potential client base" (submission by the British authorities). According to evidence from Finland, "ICT platforms, especially forum-based advertisement sites, are the main *modus operandi* regarding marketing and contacting clients in the context of THB". The French authorities report that the Internet was used by 65% of identified victims of sexual exploitation in 2019; this was up from 49% in the previous year. One key issue highlighted in the submission by the British authorities – and echoed in others – is that "advertisements that are created by traffickers are lent legitimacy by their appearance alongside advertisements that are created by autonomous sex workers". According to the Finnish authorities, "THB victims and non-victim sex workers both use the same sites". It is often very challenging for authorities to sort advertisements linked to THB from those posted by independent sex workers (see also Chapter 2).

Technology can be used to **coordinate activities during the exploitation stage**, as well as to establish contact with potential customers (including negotiating prices, determining locations and making agreements). Crucially, **technology allows for a separation** between the place where the sexual activity is performed and the place where coordination takes place. This has important implications for law enforcement. For instance, the authorities of Bosnia and Herzegovina have presented evidence of a ring exploiting Bosnian women performing sexual services in Germany and Austria – such services were coordinated and managed by offenders based in Bosnia and Herzegovina. This includes activities such as managing the victims' online profiles and scheduling meetings with clients. Evidence from France points to the presence of platforms handling calls and managing appointments remotely from Cyprus (for Russian-speaking networks) and China (for Chinese-speaking networks). In a number of cases reviewed by the Swedish police in 2019, there were "suspicions that the prostitution activities were organised by criminal networks based in the women's countries of origin, or through affiliation with an agency in a third country". The same report also identified images of different women linked to the same or very similar e-mail addresses and/or to the same mobile numbers. The authorities took these as red-flag indicators. The Swedish authorities have also come across cases of illiterate Nigerian and Romanian women who had a profile on

ASWs. This suggested that such profiles were written and managed by someone else – another potential red flag.

Countries have provided evidence of technological tools used by traffickers to **monitor and control victims** during the exploitation stage. In a case reported by the Slovenian authorities, traffickers required victims to report online on each service provided. Victims were also required to report on other victims so that traffickers could have full control over their activities. In other cases, specific apps were used to track the position of a victim.

Finally, besides the two 'main' areas of recruitment and exploitation, there is evidence of technology being used to assist with the logistics of trafficking, including the purchase of plane tickets as well as, in some instances, obtaining fake travel and other documents (evidence from Cyprus). Apps and websites can also be used to book properties in which sexual services are performed (evidence from France, Estonia, UK and Spain). While part of THB, such activities are ancillary to the two core activities of recruitment and exploitation.

As **emerging trends** in the context of sexual exploitation, there is the increase in **live streaming** of sexual performances carried out by trafficked victims. While live streaming is often connected to child sexual abuse, a handful of countries have suggested that such live streaming might also involve adult victims of THB. The Cypriot authorities have noted the expansion of live web cams. According to the Spanish authorities, traffickers are "increasingly" using video streaming webpages to market services provided by THB victims. Similarly, the the Irish authorities noted the rapid growth of so-called 'pay-as-you-go' video chat applications, such as Escortfans and Onlyfans, which are replacing traditional website platforms, providing a facility to view escorts in private or public video chatrooms. The Irish authorities maintained that "the nature of these apps and websites made it nearly impossible to know if someone is using the platforms voluntary or being exploited" (a similar trend is noted in Finland). This market segment has reportedly "expanded exponentially" since the outbreak of Covid-19. As noted by the Dutch authorities, the number of platforms "is expected to increase even further in the (near) future". This trend extends to dating sites and apps, sex advertising websites as well as social media that do not primarily focus on sexual services but can used to this end.

The Cypriot authorities have also noted an increase in the use of apps to control victims, e.g. the use of automated messages sent to a trafficker's mobile phone every time a victim carries out a specific action (e.g., opens a front door). The Swiss authorities have similarly indicated the detection of location services apps on the phone of victims, possibly downloaded without their knowledge. A similar trend in using technology to control victims has been identified in Austria. Additionally, the Greek authorities have reported an increase in the recruitment of migrant children into sexual exploitation through mobile technologies.

A few countries have reported an **increase in online interactions** due to the Covid-19 pandemic, thus increasing the opportunities for traffickers to establish contact with vulnerable individuals. The Romanian authorities have noted an increase in the number of victims recruited online in recent years, and particularly following the Covid-19 public health measures. However, they added, in Romania the majority of victims continue to be recruited via direct contact by friends, partners and relatives. In France, the authorities noted a shift from street-soliciting to "a more discreet" system based on Internet advertisements following

the Law of 13 April 2016 criminalising the purchase of sexual services. They further noted an acceleration in this process following the Covid-19 pandemic. According to the Swedish Prosecution Authority, Internet usage in relation to trafficking for sexual purposes is so pervasive that there is now "hardly any trafficking case in which Internet does not appear" as part of the traffickers' *modus operandi*. The Belgian authorities expect to see an increase in cases of vulnerable children or young adults recruited via ICTs for the purpose of sexual exploitation – as people in these age groups are increasingly interacting online and via ICTs (in an ever-changing technological landscape that is challenging for investigators to navigate).

1.1.2. Trafficking for labour exploitation

Evidence provided by State Parties indicates that, in the context of trafficking for labour exploitation, ICTs are mainly employed to **recruit** victims. According to the German authorities, Internet and social media are playing an "increasingly important role in connection with the establishment of contacts and recruitment in the area of THB and labour exploitation". This view is shared by the Spanish authorities, according to which online recruitment for labour exploitation "is becoming increasingly common". This process has probably been accelerated by Covid-19 and the resulting growth of online spaces replacing face-to-face interactions and meetings. As pointed out by the Irish authorities, "this growing use of social media to recruit migrant labourers creates an increasing challenge for authorities fighting misleading and exploitative recruitment online". According to the French authorities, while "traditional forms of recruitment (advertisements in newspaper employment sections, classified ads, flyers, word of mouth, etc.) still seem to be predominant, the use of online advertisements is growing". This is linked to the large increase in the use of ICTs by the job seekers.

Evidence of **misleading/fake job advertisements** in the context of recruitment for labour exploitation has been provided by several countries, including Austria, Croatia, Cyprus, Estonia, Finland, France, Greece, Latvia, Lithuania, Republic of Moldova, Norway, Poland, Portugal, Romania, Sweden and Switzerland. The Bulgarian authorities have highlighted the presence on various job-finding websites of advertisements in which an "employer" promises large salaries, free transport, free accommodation and bonuses for jobs that do not require high skills or fluency in the local language. Such advertisements are often part of the *modus operandi* of traffickers seeking to recruit workers to be then employed in exploitive conditions. This is echoed in the evidence provided by the German authorities according to which "some perpetrators initially offer employment on various Internet portals. The jobs are supposed to be well paid and the working hours are supposedly regulated". However, once they arrived in Germany, the workers "neither received an official work contract nor were they remunerated as promised. They often do not receive any wage at all or only a fraction of the promised remuneration". Similar advertisements have been identified in Spain, where "many victims of human trafficking for the purpose of labour exploitation are recruited through internet advertisement sites", according to the authorities.

There is evidence from the UK of fake recruitment adverts circulated on social media promoting job opportunities for highly paid labour/construction job in London – in reality, as pointed out by the authorities, "this is often not the case and no job exists". As to the content of the advertisements, the British authorities noted that "the majority of recruitment advertising reported as used by THB offenders is based on vague promises of good work, pay

and conditions, without stating specific forms of work or rates of pay. However, in a minority of recorded cases, recruitment advertising does contain these details. In labour exploitation more than sexual exploitation, it is common for the sector of work to be described, although deception is also reported regularly". Offenders can go a long way to create the pretence of legitimacy behind which they can hide their true nature: "Offenders who own businesses in which exploitation occurs also use internet enablers that mirror legitimate operators in the same marketplace, using services directories and mapping services to highlight opening hours and services offered" (evidence from the UK). There is evidence from multiple countries indicating that advertisements tend to be placed on "well-known advertisement websites" both in the country of origin of the victim (evidence from Lithuania) and in the country of exploitation (evidence from France and Greece), Another *modus operandi*, highlighted in the submission by the British authorities, consists in offenders using "Internet platforms to identify roles or vacancies in which to place victims, and to establish bank accounts to receive wages" (this is the so-called "non-employer model").

Different jurisdictions might interpret THB for labour exploitation in different ways, and the boundaries between THB, labour abuses and non-compliance with regulations can be blurred and may vary from country to country (conceptually, those can be placed on a continuum of severity starting from non-compliance with regulations to situations in which passports are taken away and freedom of movement is severely restricted). For instance, the British authorities noted that some adverts openly reference rates of pay below the national minimum wage; however, "it is highly likely that these [adverts] relate to labour abuses and non-compliance with regulations, rather than THB". Traffickers might "avoid committing to any rates of pay, which also avoids the potential of attracting attention from law enforcement and regulators". Once more, this goes to show the difficulties that authorities face in identifying and delisting such advertisements.

Advertisements are not only published on classified job websites, but also posted and circulated on social media, for instance in **specialised job-searching groups and mutual aid groups** (e.g., "Bulgarians living abroad" or "Nguoi tim viec", Vietnamese for "people looking for work"). Several countries have highlighted the relevance of pages meant to foster information exchange among migrant workers as a recruiting space targeted by traffickers – a space that is often poorly regulated as such pages might be run by individuals or poorly resourced associations. In some cases, such advertisements can be circulated via job-search groups created in messaging applications such as Telegram.

Advertisements may contain highly misleading information on working conditions and remunerations, and often the possibility of contacting the 'employer' or 'agency' only via encrypted apps such as Viber or WhatsApp. Such posts can reach a wide audience at very little (or zero) cost. In a social experiment, a Bulgarian NGO posted a job advertisement on a Facebook page offering work in Denmark in 'green roe harvesting' (a pun originating from the Bulgarian idiom "to send someone for green roe", meaning to send someone on a wild goose chase), at exceptionally high wages per hour. Within less than a week, more than 150 applicants submitted their CVs. As noted in several submissions, the level of technical skills required to leverage on online resources and social media for trafficking purposes is relatively modest and similar to the skills most web users would normally possess (incidentally, this is a far cry from sophisticated hackers and cyber-criminals).

According to evidence from Bulgaria, advertisements are often related to jobs in agriculture (seasonal workers), at construction sites, in factories and the hospitality sector. Other sectors that are considered as at risk are domestic services and care services. The German authorities have identified online advertising in the following sectors as at risk: seasonal agricultural work, cleaning services, ethnic restaurants, construction, food processing industry, transport and beauty care (nail and massage salons). The Portuguese authorities have reported several cases linked to highly misleading/fake advertisements for jobs in the agriculture and construction sectors. The Swedish authorities have flagged up cleaning services, construction, restaurants and nail salons. Further, the Cypriot authorities have flagged offers of fake educational opportunities in private universities and colleges.

As an **emerging trend** in the context of labour exploitation, the Bulgarian authorities have reported a rise in cases of recruitment through the Internet and social networks. This is believed to have been accelerated by the outbreak of Covid-19 and the related public health measures. A similar increase in advertisements on social media has been detected by the Cypriot, German and French authorities, among others. In France, the authorities have started to note the use of community-based self-help groups to recruit and control victims and to transfer funds. Finally, France and the UK have highlighted the increase in opportunities to exploit victims connected to the 'gig-economy', as identification documents are not regularly checked and individuals can work on someone else's account. For instance, a third party can receive all wages in their bank account and only pass a fraction on to the worker. According to the British authorities, "this *modus operandi* has been identified as facilitating labour abuses and illegal working, but the level of control that an account holder has over a worker's finances provides an THB risk". This view is shared by the French authorities, which noted that "although no case of trafficking has been formally detected for the moment, some self-employed workers are said to organise forms of exploitation by subletting their account to irregular migrants, making them work without remuneration or with very low remuneration". Finally, the Belgian authorities noted that it is possible to acquire forged documents on groups advertising their services on encrypted communication apps; such documents can then be used to facilitate labour exploitation (e.g., forged identity documents and driving licences, fake work contracts and fake work permits).

1.1.3. Dark Web and cryptocurrencies

Overall, State Parties have reported no evidence of significant usage of the Dark Web in the context of THB. The limited evidence presented only relates to the dissemination of child sexual abuse materials. There is some evidence from France of traffickers buying credit card details on the Dark Web and then use them to reserve rooms in hotels and rental apartments – however, this activity appears to be rather limited and ancillary. The Norwegian and French authorities have noted that live-streamed sexual abuse can take place on the Dark Web, however it is not clear from the evidence provided whether these live-streams mainly involve children or also include adult victims. Overall, it is very likely that the Dark Web plays a very limited role at the moment, since both during recruitment and exploitation traffickers seek to reach out to the largest possible audience – and this is hardly compatible with the Dark Web in its current set up and usage levels. Platforms with a large number of users are preferred for recruitment (indeed, one of the key advantages of technology is the ability to reach out to

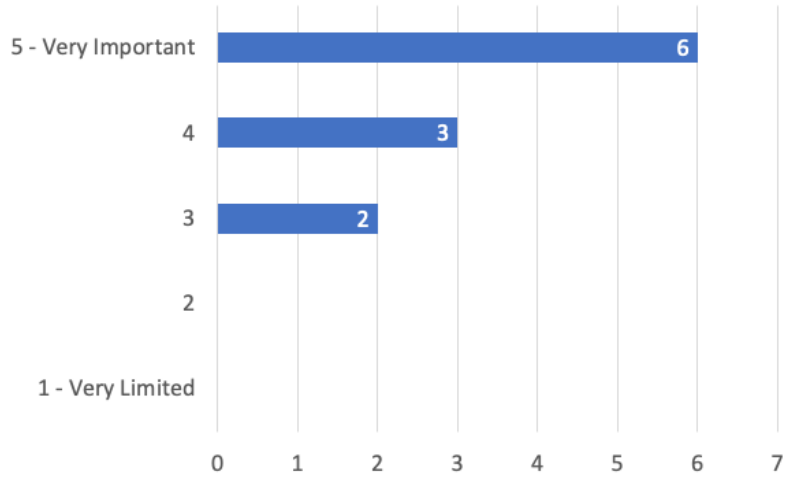
a large set of individuals at relatively little cost). Similarly, online advertisements of sexual services require contact with a large audience – something that it is not possible in the more secretive Dark Web.

Cryptocurrencies appear not to be widely used in the context of THB (on the contrary, there is evidence of their use to purchase live streaming of child sexual abuses on the Dark Web). Money transfers are still carried out using traditional methods, e.g. through companies such as Western Union or MoneyGram, or, in some cases, by using individuals (so-called 'mules'). In some instances, informal money transfer systems, such as Hawala, can be used. Some countries have started to detect money transfers via messaging apps (e.g., WeChat). It is likely that fintech products, e.g. app-based transfers, might play an increasing role in the future – as they develop a larger footprint in the wider society (similarly for crypto-currencies, once – and if – they achieve a larger circulation). Finally, there is evidence of the use of cards and vouchers that do not carry personal information (such as PaySafe cards) to pay for online services, e.g. advertising space on adult services' websites.

1.2. Evidence from NGOs

Three in four NGOs consulted for this study consider the impact of technology on THB to be either 'very important' or 'important', with no NGOs indicating a 'limited' or 'very limited' impact (Figure 2).[5]

Figure 2. Impact of technology on THB: NGOs



Note: N = 11

Overall, the qualitative evidence submitted by NGOs that directly provide assistance to THB victims paints a similar picture to State Parties. NGOs have identified the use of the Internet and social media in all phases of human trafficking, and particularly in relation to (a) recruitment; (b) exploitation; and (c) exerting control and pressure over the victims. It is a

[5] One NGO has not provided an answer to this question.

widely shared view across NGOs that the impact of technology on THB has increased during the Covid-19 pandemic. However, the pandemic might have just accelerated an existing trend. As noted by KOK – a German Network of 37 NGOs running specialised counselling services for THB victims – "for some years, the counselling centres have been reporting an ever-increasing role of the Internet and social media in trafficking of human beings".

Members of La Strada International, a European NGO Platform bringing together 30 anti-trafficking organisations in 23 European countries, reported cases of THB recruited via different online platforms, including social media and dating websites, for both sexual and labour exploitation. These cases concerned the recruitment of both adults and children. According to data from CKM, a Dutch NGO, online contacts play a particularly important role when victims and perpetrators are strangers to each other: in almost 80% of these cases, the first contact is made online, e.g. via social media or dating apps (evidence provided by La Strada International). This is particularly pronounced among underage victims. Based on interviews with THB victims, the Albanian NGO "Different and Equal" noted that social media "have become the main means" through which offenders recruit victims. This is the case particularly for "girls [recruited] for sexual exploitation". In Switzerland, FIZ has also observed an emerging trend of THB recruitment via different social media platforms, as well as dating apps. Overall, there is a wide consensus on the fact that the usage – and importance – of technology in THB cases is on the rise – and that such upward trajectory has accelerated during recent years.

1.2.1. Trafficking for sexual exploitation

Strategies and mechanisms underpinning recruitment through social media reported by NGOs are in line with the evidence already discussed in Section 1.1.1 above. There is evidence of the so-called "lover boy" strategy, i.e. establishing a personal/romantic relationship via social media to subsequently exploit the victim. Fake social media profiles are set up to this end. Victims tend be to underage or young adults. La Strada Moldova noted that children from rural areas, from socially vulnerable families or with a poor financial situation are particularly vulnerable.

Mechanisms similar to those discussed earlier in this report have been highlighted by NGOs in relation to the exploitation stage. These include the use of websites to advertise sexual services. KOK (Germany) noted that it is more difficult for police and counselling services to approach individuals advertising sexual services online vis-à-vis those providing the same services in registered establishments – thus making the identification of THB cases more challenging.

Further, in the case of sexual exploitation, accommodation can be booked online via specialised sites (evidence from France via La Strada International).

1.2.2. Trafficking for labour exploitation

With respect to recruitment for labour exploitation, NGOs have provided further evidence for the mechanisms already discussed in Section 1.2.2 above, particularly on the use of fake and grossly misleading online job advertisements. For example, in Albania, the NGO "Different and

Equal" observed online job advertisements linked to exploitative practices targeting both men and women. In Serbia, the NGO "Astra" expressed concern that even agencies officially registered with the Business Register Authority and with a regular licence might be advertising unlawful jobs. They also noticed "a large number" of "unauthorized" advertisements, i.e. advertisements by individuals purported to be representatives of agencies as well as advertisements linked to exploitative practices. Most of the online advertisements, they consider, "are not subject to any form of control or supervision". Evidence of online recruitment for jobs that either do not exist or are subject to exploitative conditions has also been uncovered by German and Swiss NGOs. This is in the context of a "proliferation of online job recruitment", as pointed out by Migrant Right Centre Ireland.

There is no evidence in the submissions by NGOs of technology playing a key role in the exploitation phase in the context of labour exploitation. However, it has been flagged up that gig-economy jobs, particularly online platforms for food and other deliveries, might be vulnerable to abuse by traffickers. As noted by the French NGO "*Comite Contre l'Esclavage Moderne*" (CCEM, a French member of La Strada International), while no cases of THB have been identified so far in this context, the procedures currently implemented by online delivery platforms might allow traffickers to employ victims using someone else's identity.

1.2.3. Control and pressure over victims

NGOs noted that technology is used to exert **control over victims**, particularly in the context of sexual exploitation. There have been instances in which traffickers relied on video surveillance, mobile phones, apps and software to track locations (evidence from La Strada International). Offenders can also use ICTs to make threats to family and friends, e.g. via social media, should a victim decide to escape their condition (evidence from KOK, Germany). Similar evidence has been collected by the NGO "Astrée" in Switzerland.

Further, victims can be subject to **blackmail** using social media and other online platforms. This is often linked to a threat to divulge 'compromising' information, including pictures and other personal information (KOK reports a case of a trafficker blackmailing her victim by threatening to post her HIV status on Facebook).

Crucially, NGOs have highlighted that traffickers can use ICTs, including social media and encrypted apps, to **continue contact** with a THB victim even after the person has left the exploitative situation – often to prevent them from filing complaints and seeking justice. In the Netherlands, CKM found this to be the case in roughly one third of the victims they interviewed (evidence provided by La Strada International).

1.2.4. Emerging trends

KOK and La Strada Moldova noted an increase in the exploitation of children **via webcam and social media**. According to La Strada Moldova, offenders get in contact with children on social networks or **online games**, befriend them or simulate a romantic relationship. Sometimes offenders might pose as representatives of modelling agencies. The child is then asked to share intimate photos which are then used to blackmail them. At this point, offenders ask their victims to produce and share more sexually explicit content as well as produce live-

streaming of sexual performances. In some cases, victims are pressured to recruit other children or meet offline for sexual acts (KOK observed similar patterns).

More generally, La Strada International and KOK have pointed to the increasing vulnerabilities created by the **disclosure of large amount of personal information** on social media and other online platforms, as well as the increasing openness with which individuals might establish intimate contacts with strangers on online platforms[6]. This is more prominent among younger generations. While technology can bring considerable opportunities and advantages – including enriching exchanges – it can also exacerbate vulnerabilities. For instance, sharing sexually explicit images (sexting) might pose THB-related risks as well as risks of blackmailing more generally. While statistical data is still lacking, research commissioned by La Strada Moldova in 2020 with a representative sample of children aged 9-17 gives some interesting contextual insights. This work found that 13% of children in the Republic of Moldova consider that sharing intimate photos online is normal between people who love each other[7]; 35% communicated with strangers online and 20% met up offline with people they first met on the Internet (2% of the latter claimed they were upset by what happened at that meeting).

1.3. Further evidence from the landscape analysis

While technology might impact Trafficking in Human Beings (THB) during all its stages, its role is of particular concern in relation to two stages of the process: recruitment and exploitation (Latonero 2012; Di Nicola et al. 2017 among others).

Technology can play a role in the **recruitment** stage by facilitating the identification, location and contact of potential victims. The main change brought about by technology has been an expansion in the traffickers' reach in their search for victims, while lowering the 'operating costs' of the identification and contact of potential victims (Raets and Janssens 2018). However, as in-person follow-up interactions still play a crucial role, traffickers still face limits to their scale of operations. As different mechanisms are at play depending on the type of exploitation, it is crucial to separate recruitment for the purpose of sexual exploitation from recruitment for the purpose of labour exploitation [8].

In relation to the recruitment of victims for **sexual exploitation**, technology can assist recruitment in two ways:

a. It can facilitate the creation and dissemination of **online job advertisements** that promote working opportunities, most often abroad, in a number of sectors ranging from administration, cleaning or child care (Europol 2014) to entertainment, modelling, escort services and the sex industry (CoE 2007; UN.GIFT 2008; Di Nicola et al. 2017).

b. It can facilitate the identification of and contact with potential victims, often vulnerable individuals, via social media and other personal-contact Apps (see, e.g., Di Nicola et al. 2017).

[6] It should also be noted that social media and ICTs more generally can also help CSOs identify and establish contact with potential THB victims (more on this point in Chapter 3).

[7] Only 1% of interviewees explicitly said they had shared intimate (sexually explicit) photos and videos. This result, however, needs to be interpreted with caution as it might have been influenced by a social desirability effect.

[8] There is no evidence that technology is used in the recruitement for other types of exploitation, including forced begging.

This can be thought of as a specific type of **online grooming**. The technology-based approach is often used in the 'boyfriend' model of recruitment. The specific websites and applications ('apps') used may change depending on country-specific online behaviour and preferences. Some sources have pointed to an emerging practice of acquiring 'compromising information' during the recruitment and then blackmailing victims to obtain control (a practice similar to 'sextortion'; Europol 2020).

In relation to the recruitment for **labour exploitation**, technology mainly assists recruitment through the dissemination of online job advertisements. Specific sectors have been identified as particularly at risk: women are more likely to be recruited in relation to personal care, house care, hairdressing and babysitting while men are more likely to be recruited in relation to agriculture, construction, transportation and the collection and delivery of charity bags (Europol 2014; Di Nicola et al. 2017; see also Fine Tune Project 2011 and CoE 2007). Additional sectors identified include: catering, food processing and packaging (Fine Tune Project 2011). Advertisements can be posted on legitimate, widely-accessed websites, on ad-hoc websites and/or circulated through social media.

While certain sources appear to emphasise the physical separation between traffickers and victims achieved thanks to technology (OCSE 2020), the reality is more complex. There is strong evidence to suggest that the use of technology complements rather than substitutes personal, offline interactions. Technology and in-person interactions are best seen as integrated. It is very likely that the extent of the impact of technology depends on factors specific to certain at-risk populations in specific countries, including: (a) usage of Internet and social media in general; (b) usage of Internet and social media when searching for jobs; and (c) technological literacy of certain at-risk groups.

Research suggests that victims are normally—but not always—recruited in their country of origin and then exploited abroad. This finding was already highlighted in CoE (2007), and subsequent, albeit limited, evidence provides additional support. The implication is that bilateral and multilateral actions are likely to be required to counteract such phenomena.

Moving to the **exploitation stage**, technology can play a role in relation to sexual exploitation. However, hardly any evidence of a noticeable role of technology in labour exploitation has been found in this review (Di Nicola et al. 2017; Raets and Janssens 2018 among others).

In the case of **sexual exploitation**, technology can come into play in two different ways:

a. It can facilitate traffickers' **control** over victims through using GPS or other mobile applications, thereby limiting the need for traffickers to be physically close. Blackmail and the use of compromising information against victims have also been mentioned as possible strategies to exert control (Raets and Janssens 2018). In a rare piece of evidence, it appears that blackmailing of victims has been identified in a relatively small proportion of cases analysed in the Netherlands (8.8% of cases, undated; source: OCSE 2020).

b. It can facilitate the **sale** of sexual services provided by THB victims via online advertisements targeted to final customers. Such advertisements are often posted on specialised websites or ad-hoc webpages.

Overall, the impact of technology on the **transportation** stage is seen as limited, as victims often travel voluntarily and only start experiencing coercion when reaching the destination country (exploitation stage; evidence from law enforcement agencies from Bulgaria, Romania and Italy presented in Di Nicola et al. 2017). The use of technology in this stage is mostly related to mobile phones and apps used to arrange travel and coordinate the time and place of meetings, as well as the use of the Internet to purchase tickets and make travel arrangements. While it is possible for traffickers to use the Dark Web to purchase counterfeit tickets as well as compromised credit card details that are then used to purchase (fake) travel documents, a close assessment of multiple sources, both academic and publicly available law enforcement documents, suggests that the usage of Dark Web still appears to be very limited.

2. Challenges in detecting, investigating and prosecuting technology-facilitated THB

This chapter explores the challenges that arise as a consequence of the use of technology in the context of trafficking in human beings (THB). Broader challenges faced by State Parties that are not directly related to the use of technology are not addressed. This chapter first explores the challenges related to investigation followed by those related to prosecution and international cooperation based on evidence provided by State Parties. This is then complemented with evidence collected from NGOs, as well as through a review of the current literature.

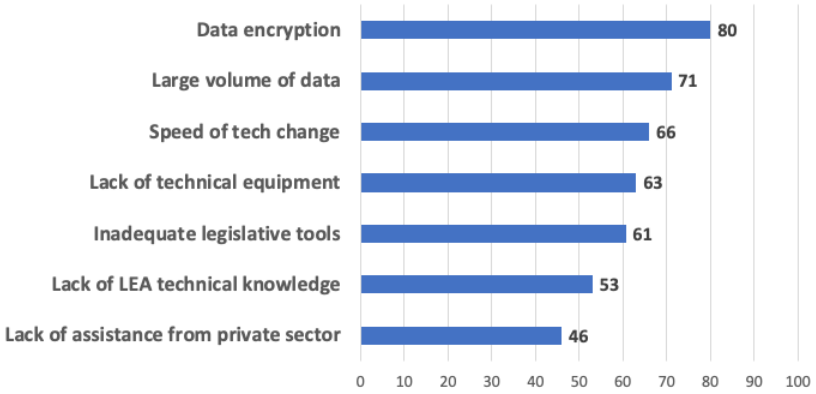
2.1. Challenges to investigation

State Parties were presented with a list of seven potential challenges to investigations identified on the basis of a review of the current knowledge base, as well as earlier works carried out by GRETA, the CoE Group of Experts on Action against Trafficking in Human Beings, and the Council of Europe, including the 2019 Workshop on "Stepping up the Council of Europe action against trafficking in human beings in the digital age"[9]. Figure 3 presents the **severity score** for each of the seven challenges[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] For each challenge, State Parties were asked to evaluate its severity using a three-point scale ("Normally not a problem", "Minor problem" and "Major problem"). Such information was then transformed into a score by assigning a value of 0, 1 and 2 to, respectively, "not a problem", "minor" and "major". Scores were then rescaled on the [0, 100] range.

Figure 3. Severity scores for challenges to investigations



Note: Scores range = [0, 100]

Data encryption is seen as the most severe challenge (score of 80). At the opposite end of the ranking, lack of assistance from private sector companies is seen as the least severe challenge. All challenges but assistance from private sector companies score higher than 50, which means that their overall impact is considered to be more than just a "minor" problem.

These challenges are assessed in turn un the following sections: data encryption (2.1.1), the large volume of data to be processed (2.1.2), lack of technical equipment (2.1.3), lack of technical knowledge among law enforcement (2.1.4) and speed of technological change (2.1.5). Challenges related to assistance from private sector are discussed in Section 4 in this chapter, while challenges arising from legislative tools are discussed in Chapter 5. It should be noted that, while discussed separately, some of the challenges are intertwined. For example, data encryption (and decryption) requires continuous investments in technology, as well as in building expertise among law enforcement personnel. State Parties were also asked to indicate any further challenges they face in addition to the seven already identified. Those additional challenges are discussed in Section 2.1.6 below.

2.1.1. Data encryption

Data encryption is viewed as the major challenge faced by authorities when carrying out investigations into ICT-facilitated THB. While the impact of TOR/Darkweb or encrypted phone networks such as Encrochat is deemed as marginal, countries have pointed to the challenges posed by encryption protocols included in widely used apps and online services (such as WhatsApp and Telegram). Data encryption can "make impossible to recover data during a forensic investigation" (Albanian authorities). The authorities of Bosnia and Herzegovina maintained that "more and more investigations lead to encrypted HHD, locked telephone devices, memory sticks and encrypted data". According to the Icelandic authorities, most problems faced by police come from "anonymous and encrypted e-mail accounts and apps, such as Proton-mail or [getting] f.ex. subscriber information". Monitoring and surveillance are also restricted, if not impossible – even with a legal warrant and contrary to other types of communications. The Austrian authorities noted the impossibility to place Internet Protocol telephony (VOIP) under surveillance while the French authorities have highlighted "the impossibility of monitoring instant messaging (Whatsapp, Messenger, Tik Tok, Wechat,

Snapchat)", thus creating "a major obstacle to investigations (difficulties in the identification of perpetrators and victims, establishing links between people, collecting evidence on coercion and subordination)"[11]. The Belgian authorities further noted that investigating activities carried out in closed encrypted channels require the use of informants and undercover agents – and this can be problematic in certain jurisdictions (including Belgium). The Irish authorities expressed the view that "encryption is growing stronger" – and this was echoed by several State Parties. The variety of encrypted technologies available to the general public is growing, with more and more instant messaging applications designed to maximise encryption and minimise the amount of user-data generated (e.g., Threema or Signal).

As pointed out in the Swiss submission, the impact of encryption varies depending on whether investigators have access to the physical device or not. If the device is physically in the hands of the investigators, then "data encryption is a minor problem, and the data can be decrypted by specialist police services" (a similar point is made by Luxemburg). However, officers with these technical skills are scarce and these services are likely to be overwhelmed – therefore adding delays to an investigation. If law enforcement agencies do not have access to the physical support, then "investigations are more difficult" (Swiss submission). In some countries, for example the United Kingdom, police forces have the power to request a person to hand over their mobile phone password or PIN. However, as the British submission of evidence points out, problems do remain: "even on arrest and seizure of such devices, there may be barriers to accessing important communications", particularly from devices with high level of security features. This was echoed by the Belgian authorities, noting difficulties in decrypting the most sophisticated algorithms (they thus called for more investments in new decryption tools).

A few countries have hinted at the existence of tools to decrypt at least some types of algorithms. It is clear, however, that this is a constantly evolving landscape which calls for (large) investments in both training and software. Steps taken to overcome this issue include the establishment of cybercrime units/centres tasked with working on decryption technology. This is the case for Norway, for instance. Similarly, France is currently working on developing a password cracking device "at the central level".

The Slovenian authorities have raised the issue of costs related to decryption of electronic data. Such costs are generated by the need to hire specialised, highly trained personnel, as well as buying specialised pieces of software that are able to circumvent encryption. Furthermore, as encryption protocols evolve incessantly, there is a need to keep the software constantly up to date, which often comes with hefty licence fees.

Further, there could be value in sharing resources at the supranational level in the development of technological products, such us decryption software and web-crawlers as suggested, for example, by the Swedish authorities. Overall, it transpires from the evidence submitted that more can be done in **fostering knowledge exchange and pooling tech development** across countries. Closer and adequately funded technical cooperation has proven to be highly successful, for instance in the infiltration of the encrypted messaging network Encrochat used by high-level organised crime groups across Europe (this has led to

[11] This is echoed in the submission of evidence by the Greek authorities.

multiple high-profile investigations and trials in France, the Netherlands, the UK and Sweden, among other countries).

In some cases, as pointed out by the French authorities, encryption can be overcome by using alternative investigative techniques, for instance through "technical surveillance of victims' telephone lines [which] remains an effective means while waiting for a technology that will make it possible to bypass encryption".

2.1.2. Large volume of data

Electronic communications and ICT devices generate an incessantly growing volume of data, which, in turn, can pose substantial strain on investigators. As pointed out by several countries, the large volume of generated data has an impact on the ability to extract them, requiring powerful technical equipment. Equally challenging is the analysis and careful scrutiny of large quantities of information. Smartphones have ever larger storage capacity; user-generated evidence can come under multiple forms: (long) chats, but also images, film recordings and voice messages that can take "weeks" to be analysed (evidence from Switzerland). This challenge is particularly exacerbated in cases where "no specific keyword search can be carried out and [investigators] have to sift through all the data" (evidence from Switzerland). According to the Swiss authorities, "experience and practice have shown that the amount of data has increased massively with modern social media, potentially generating very long investigation activities […] which can keep an investigator busy for months and cause resource bottlenecks".

The large volume of data often calls for specialised pieces of software, as well as specific training on how to systematise and search within such large bodies of evidence. According to the British authorities, "Internet marketplaces and social networks generate an enormous amount of data [which] can be difficult to parse, and it is expensive to license or develop tools that can effectively analyse this information". The French authorities have equally stressed the need to develop tools able to assist investigators in handling large-volume data, for instance by using Artificial Intelligence (AI) algorithms (a similar point was made also by the Spanish authorities). According to the Norwegian authorities, the volume of electronic data makes "investigations more complex with the need for more technology-based investigative methods"[12]. Such methods, however, often "lead to a high volume of data [of which] only a small part […] is useful for the investigation".

There is broad consensus on the fact that building capacity in handling large amount of electronic evidence is crucial. However, such capacity needs to be constantly updated to keep pace "with constantly shifting Internet enablers due to the speed of technological change" (British submission). This is echoed by the Dutch authorities, which highlighted the growing amount of data generated by online platforms and social media, as well as the challenge posed by **changing behavioural patterns** of their users, making it "difficult to find out where to search". Availability of digital tools is seen as the first (necessary) step; however, constant adaptation to the technological and behavioural digital environment is the challenging yet necessary further step.

[12] The Portuguese authorities have made a similar point.

To compound the problem, large volumes of data often need to be processed and analysed within a short timeframe. For instance, when a suspect is placed under arrest, officers are under time pressure to review large amount of electronic evidence very quickly – as pointed out by the Slovenian authorities. The limited amount of time often available to investigators to review the material calls for "**better technology to search and sort the information**" (evidence from the UK). Moreover, several State Parties have highlighted that electronic data collected in the context of THB investigations are often in a language that is not normally spoken by the investigators, thus requiring long and costly translations (this issue is particularly acute among destination countries).

2.1.3. Lack of technical equipment

Several countries have highlighted the lack of technical equipment as a major challenge to investigations. This includes an often insufficient number of machines able to perform specialised tasks, such as breaking encryption, as well as difficulties in keeping up to date with software and hardware developments. As already discussed above, specialised software and hardware can come with hefty price tags, and often require constant updates and expensive licensing agreements to keep up with the speed of technological change. This can have a considerable impact on police budgets. Countries with less purchasing power find it hard to keep up with requirements in terms of technical equipment. Had it not been for the support of international partners and private sector donors, some countries would have been already priced out of the international market for specialised technical tools (this point is explicitly made by the Albanian authorities, but it transpires from other countries' submissions too). However, this is by no means an issue restricted to less resourced countries. Germany, Belgium, Sweden, France and the United Kingdom, among others, have expressed serious concern about the cost of specialised software and hardware equipment.

Most cases of THB are international in nature, and often involve victims from less affluent countries being exploited in more affluent nations. This generates a need for international cooperation among countries over specific cases. It also translates into an often neglected need for strengthened technology-assistance programmes supported by destination countries for the benefit of source countries (i.e. the victims' countries of origin) – in addition to the existing multi-lateral programmes, such as those ran by the European Union that are already providing financial support for upgrading technological equipment.

2.1.4. Lack of technical knowledge among law enforcement

Technical equipment alone is of limited use if there is no adequate training available to law enforcement agencies. More generally, investments in human capital, i.e. in training and technical knowledge among police officers, are as important as those in software and hardware – if not more. The need to provide such training and further technical knowledge of police officers has been widely mentioned by State Parties. In the words of the Belgian authorities, it is "imperative" to reduce the "**digital divide between offenders and police forces**". A variety of knowledge needs have been identified by State Parties.

Firstly, there is a need to develop knowledge on the emergence of new trends and changes in the use of technology by both offenders and victims. Secondly, countries have highlighted the importance of developing knowledge on the emergence of new apps and services in a tech market that is characterised by rapid change. Thirdly, there is a need to keep up to date with the development of new security protocols and encryption methods. Crucially, knowledge needs to be distributed cleverly within an organisation. For instance, the lack of specialist officers at the local level can create **bottlenecks in the investigations**, if assistance from a (busy) centralised unit needs to be repeatedly sought. This is a crucial issue that countries should pay adequate attention to – and that was evidenced in the submission from several State Parties, including Albania, Belgium, Iceland, France, Portugal, Slovakia and Slovenia (please refer to Chapter 4 for a more in-depth discussion on training).

Several countries have highlighted the need to **provide additional technical training to 'general' police officers**. Besides training specialised officers with high-level technical knowledge related to specific pieces of software or decryption techniques, there is a need to provide a basic set of digital skills and tech knowledge to all officers. It is crucial that officers that first intervene in a crime scene possess such knowledge. As noted by the Albanian authorities, mistakes made by first respondents "can be fatal in collecting electronic evidence, [which] then becomes invalid for further analysis". Adequate training on acquisition and handling of **electronic evidence** needs to be provided to the largest number of officers. Moreover, developing expertise in this domain should be made a regular topic in the training curricula for police officers.

Additionally, while a basic level of technical knowledge would be a real asset for all investigators, there might be more complex cases in which teams with multidisciplinary skill sets might need to be set up (e.g., by bringing together investigators, financial and cybercrime specialists). Countries might wish to consider introducing – or enhancing – provisions facilitating a swift constitution of such teams, whenever needed, or even making interdisciplinary teams a more structural feature of modern police work. This could be extended to international joint investigation teams, e.g. by including technology and communication experts in such teams (a point raised by the Bulgarian authorities).

The Swiss authorities note that "keeping pace with technological progress is a major challenge for law enforcement", and today's investigators require expertise in both human trafficking and ICTs, including social media usage and technical skills. The French authorities have expressed the need to train more staff in new technologies, as well as in financial investigations. The Bulgarian authorities have reported an example in which a mix of online and offline investigative techniques were employed in cooperation with the French authorities. Moving from the discovery of pornographic images of children, investigators were able to first identify the IP address and then physically locate it to an hotel. While swooping on the hotel, they found a number of women forced to offer sexual services and obtained a series of Facebook nicknames of other victims, who were then identified using their Facebook profiles. In the end, 60 victims of trafficking for sexual exploitation were identified, one child victim coerced to produce pornographic material and 18 offenders. This case points to the need for investigative officers to be well-versed in both online and offline investigative techniques, as it is increasingly likely that both will need to be leveraged on during THB investigations. This, of course, would require continuous training.

2.1.5. Speed of technological change

The fast pace of technological change is a cross-cutting issue that has an impact on all the challenges discussed above: encryption, training of police officers, technological equipment and collection of electronic evidence. Please refer to the discussion above for further details.

2.1.6. Additional challenges to investigations

A number of countries have flagged up an issue related to the (inadequate) **data retention obligations** imposed on Internet Service Providers (ISPs), and its impact on investigations. In Bulgaria, for instance, the current legislation requires ISPs to store such data for six months – a length that is considered inadequate for building strong investigations. The length of data retention periods was also raised by the Dutch and Maltese authorities. The Norwegian authorities have noted that, under domestic legislation, ISPs are not allowed to store information about IP addresses for more than 21 days and they are not required to store the information on the link between a subscriber and an IP address. The Bulgarian and Romanian authorities have called for an harmonisation of national regulations regarding the storage of Internet traffic data, as well as investigation practices related to ICT-facilitated offences.

The prohibition of Trojans (i.e., spywares) is regarded as an additional challenge for ICT-assisted investigations as law enforcement agencies are not allowed to enter homes and other premises to install spyware on devices used by individuals under investigation. Authorities maintain that such tools would allow law enforcement agencies to mitigate issues related to encryption, as well as the difficulties in eavesdropping on VOIP conversations. The Belgian authorities have called for changes in the legal framework to facilitate investigative work using new technologies. They noted the need for simplification of procedures and legal tools taking into account the offenders' *modus operandi*.

The Bulgarian authorities have raised an issue related to electronic evidence, specifically the need to introduce international requirements for ISPs to implement appropriate security protocols preventing any **tampering with the data** both during storage and transmission to law enforcement.

The Dutch authorities have raised an issue linked to the application of **privacy laws**, for example in the context of using a web crawler.

The Spanish authorities have called for more personnel specialised in both THB and advanced computing skills. The Belgian authorities have made a similar point.

The Moldovan authorities have highlighted difficulties in retaining skilled practitioners as officers with experience often leave specialised units to join other parts of the judiciary or the private sector, and have stressed the importance of regular motivation reviews to attract and retain talent.

The Austrian authorities have highlighted an issue with the penalties envisaged for THB in their domestic Criminal Code, which ranges between six months and 10 years' imprisonment. While this penalty is sufficient for a court-ordered surveillance of messages, it does not

authorise police forces to employ visual and acoustic surveillance (i.e., audio surveillance of private conversations and private premises).

The British authorities have noted a challenge around IP addresses and electronic evidence. IP addresses are a starting point in an investigation and, once obtained, law enforcement needs to match those IP addresses to various screen names and users. However, screen names can be changed at any time and are often used by suspects interchangeably. It is crucial then for law enforcement to check the continuity of IP addresses to screen names. Additionally, in virtual chat rooms, some users can be seen on the screen -- and their identities proven – but there may be others who do not have their webcams on. Some suspects may share devices with others, for instance if they are in a multi-occupancy home, which, in turn, might make their identification challenging.

The British authorities have also raised the issue of dealing with unused electronic material, particularly in the context of GDPR obligations. On the same line, the Dutch authorities consider that the international data protection regulations "hinder the gathering, storing and processing of information obtained with technological investigative techniques (such as web crawling)", thus "preventing the optimal use of [such] techniques".

ZOOM | Challenges in detecting cases of ICT-facilitated THB

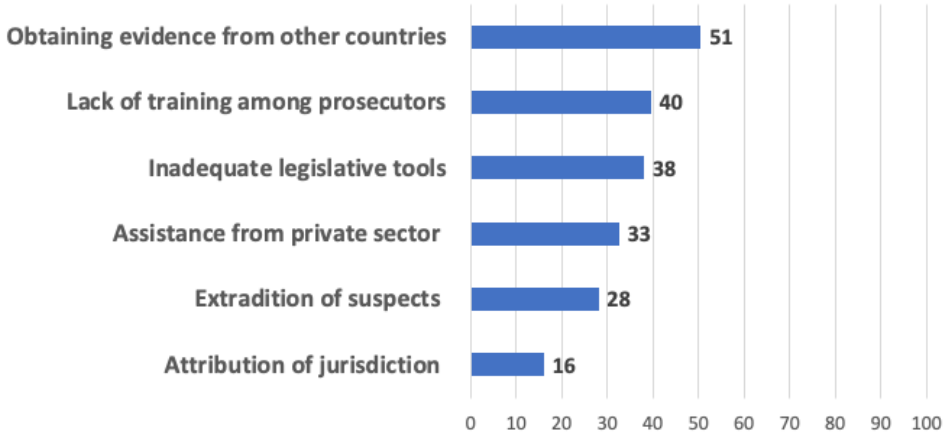
Investigations and prosecutions are contingent on cases being detected in the first place. Below are the challenges identified by countries related to the *detection* of ICT-facilitated THB:

- Internet constitutes a very large space to monitor, and the volume of online activities/interactions is constantly growing. Online resources span a very wide and diverse spectrum from online advertisement sites and adult websites to social media platforms, chatrooms and potentially the Dark Web. Policing such a space is very resource intensive and subject to legal restrictions (privacy laws and limitations to the use of web crawlers in some countries).
- Manual search of online websites is extremely challenging while large amounts of unstructured data make web-crawling difficult (if at all allowed by domestic legislations). Volume of online advertisements (open and classified) for both sexual and non-sexual services is often too vast to be manually searched.
- Difficulties in identifying both perpetrators and victims as they may use nicknames and aliases when operating online. Anonymising software (e.g., VPNs) and the use of encrypted communication between traffickers and victims further hinders identification. Conversations between traffickers and victims take place in closed groups (e.g., Facebook, WhatsApp, Telegram).
- Fast-changing behaviour of Internet users (e.g., new technology emerges, new websites/apps become popular in a short time). In addition, new tools rapidly emerge, boosted by strong competition in the tech sector, which may provide traffickers with new means to connect with and exploit victims.
- Challenges in sorting online advertisements to identify those related to THB –in the context of both sexual and non-sexual services. Advertisements for sexual services provided by victims of THB often use the same sites, terminology and wordings as those posted by independent sex workers. 'Red flags' to identify advertisements related to labour exploitations are still underdeveloped or not consistently utilised.
- Absence of specialised units within the police and/or lack of specialised THB investigators with advanced computer skills. Lack of officers trained to carry out covert operations on the Internet (e.g., by creating and maintaining a 'fake' profile).
- Lack police officers' training on the specificities of ICT-facilitated THB (e.g., offenders' *modus operandi*, platforms on which it occurs, how to covertly approach traffickers and create credible online profiles).
- The possibility to remove/alter conversations (electronic evidence) by traffickers.
- Time-consuming process of sending requests to social media companies (often based in a foreign jurisdiction) and lack of response from some companies.
- Short data retention periods for IP addresses and difficulties in accessing them.
- Language barriers.

2.2. Challenges to prosecution

State Parties were presented with a list of six potential challenges to prosecution identified on the basis of a review of the current knowledge base, as well as earlier works carried out by the Council of Europe, including the 2019 Workshop on "Stepping up the Council of Europe action against trafficking in human beings in the digital age"[13]. Figure 4 presents the **severity score** for each of the six challenges[14].

Figure 4. Severity scores for challenges to prosecutions



Note: Scores range = [0, 100]

Overall, challenges to prosecution score lower than those to investigation, with only "obtaining evidence from other countries" scoring slightly higher than 50 (scores higher than 50 indicate that the challenge is broadly perceived as more serious than just a 'minor problem'). This is likely due to the fact that, if a case has indeed arrived at the prosecution stage, most hurdles have been successfully cleared during the investigation stage.

Below, we offer some further qualitative evidence on three challenges: attribution of jurisdiction, extradition of suspects and training of prosecutors. Challenges related to assistance from private sector are discussed in Section 2.4, while challenges arising from legislative tools are discussed in Chapter 5. Challenges related to obtaining evidence from other countries are discussed in the Section 2.3, which presents the obstacles to international cooperation.

- *Attribution of jurisdiction*: While, overall, the attribution of jurisdiction is seen a minor challenge among State Parties, occasional issues might arise in ICT-enabled cases regarding concurrent jurisdiction. In some cases, challenges might arise in the identification of suspects

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

[14] For each challenge, State Parties were asked to evaluate its severity using a three-point scale ("Normally not a problem", "Minor problem" and "Major problem"). Such information was then transformed into a score by assigning a value of 0, 1 and 2 to, respectively, "not a problem", "minor" and "major". Scores were then rescaled on the [0, 100] range.

and, crucially, their location, meaning linking a specific IP address to a person and then that person to a location in a specific jurisdiction.

- *Extradition of suspects*: Overall, this is seen as a relatively minor issue. The European Arrest Warrant (EAW) and the European Investigation Order (EIO) are considered two important tools that have "made it possible to respond effectively (and also with some speed) to the challenges posed by transnationality" (Portuguese authorities). The work of Eurojust has been mentioned as an example of good practice. The Swiss authorities have highlighted the obstacles they face by not being able to issue EAWs and EIOs. Similarly, the British authorities have indicated that the "UK's exit from the EU may impact on extradition" as "nationality bar from some countries means that [the UK] can no longer extradite some EU nationals and requires discussions on which country prosecutes". Differences in trafficking legislation between countries might create challenges in extraditing suspects.

- *Training of prosecutors*: A few countries highlighted the importance of adequate training for prosecutors on ICT-facilitated THB, noting that in some cases this training is lacking or not adequate. Training of prosecutors is seen as key to ensure that ICT-facilitated cases are robust, that electronic evidence is properly collected and utilised, and that cases (and the evidence therein) are adequately presented to a judge/jury. Some countries, such as Norway, are planning to step up such training by having a prosecutor with experience of THB cases giving lectures to colleagues. Furthermore, expertise may not be consistently available across all prosecutors' offices in a country. This issue was noted, among others, by the Dutch authorities. As a response, the Dutch prosecution service, together with the national police, is currently assessing the level of expertise across the service. Such an intra-State monitoring process can be seen as an example of good practice to ensure consistency in the level of expertise within a jurisdiction. Further, some State Parties have noted instances in which prosecutors were not familiar with the procedure to request electronic data from private companies; in other instances, prosecutors were not familiar with procedures to obtain evidence and cooperation from other countries, for instance by setting up a Joint Investigation Team or issuing a European Investigation Order. Enhanced training for prosecutors should ease the process of liaising with other countries as well as private companies. Finally, State Parties have expressed the view that interdisciplinary training with elements of both THB and ICT should be extended to judges.

Furthermore, State Parties were asked to indicate any **additional challenges** they face in prosecuting ICT-facilitated THB cases. Below is a summary of the challenges identified:

- The British authorities have flagged an issue in proving participation and *mens rea* of individual offenders in ICT-enabled cases when there is group activity, for example in an internet chat room where one screen may be showing abuse of a trafficked victim while other screens may be showing other users engaging in consenting adult activity. Proving the participation of different individuals can be challenging given the different roles involved.

- A further challenge highlighted in the submission by the British authorities relates to the presentation of evidence in front of a jury (or judge). In ICT-facilitated cases, the presentation of technical evidence is often delivered from an expert familiar with the technology (explaining how, for instance, live streaming from internet chat rooms works, its functions, and what recordings may have captured, including a description of what a recording

show). Developing in-house expertise among officers on how to effectively and accurately present electronic evidence may be increasingly valuable. A connected challenge relates to the presentation of large volumes of electronic material to a jury. A solution being explored in the UK is the use of tablets.

2.3. Challenges to international cooperation

The study asked State Parties to indicate the challenges they face in relation to transnational investigations and judicial cooperation in the context of ICT-facilitated THB. Most of the challenges highlighted are not specific to ICT-facilitated THB but affect cross-border investigations and judicial cooperation more generally, e.g., language barriers, different legal basis, coordination of parallel investigations, swift exchange of information. However, the specificities of ICT-facilitated THB often exacerbate them. This is particularly acute in the case of electronic evidence. In addition, in the context of ICT-facilitated THB, receiving mutual legal assistance and securing evidence are often time-critical.

2.3.1. Mutual Legal Assistance Requests

The lengthy turnaround for the processing of Mutual Legal Assistance Requests (MLAs) has been flagged up by the majority of State Parties as one of the major obstacles to international cooperation. Overall, mutual legal assistance procedures are seen as slow, sometime unpredictable and in need of internationally agreed unified templates. As noted by the Spanish authorities, "too many sources of information require judicial authorisation for their access". Such requests have to be processed through MLAs, which, in turn, complicate and lengthen investigations. The current system has been described as 'inadequate' by several countries. MLA requests between CoE State Parties can take place within two distinct scenarios: (a) within the EU framework of judicial cooperation (including through the assistance of Europol and Eurojust) and (b) outside the EU framework. As challenges and procedures can be radically different depending on the scenario, it is important to discuss them separately.

*Cooperation within the EU legal frame*work. CoE State Parties that are also members of the European Union perceive the EU coordinated framework of police and judicial cooperation as beneficial and able to smoothen the process. This includes the work of EU agencies such as Eurojust and Europol. However, challenges still exist. According to the French authorities, "international cooperation tools, although interesting, are slow: a European Investigation Order (EIO) takes several months and a Joint Investigation Team (JIT) is difficult to implement". One major obstacle to the implementation of JITs is the need for a mirror investigation in the other country(-ies). This was also noted by the Norwegian authorities.

Cooperation outside the EU legal framework. This is seen as a more time-consuming process and characterised by greater intricacies than in the scenario above due to the lack of harmonisation among different legal systems (as pointed out, among others, by the Cypriot and Spanish authorities). Swiss authorities have noted that the response to "requests for international legal assistance often depends on the goodwill or interest of foreign prosecutors". This introduces an element of unpredictability and inconsistency in the process. Such "negotiations between prosecutors' offices are often lengthy". **Clearer operating**

procedures, enhanced regular exchange among contact points and requirements for MLAs clearly set out and discussed at the outset would help smoothen the process. The authorities in North Macedonia noted that all MLA requests need to go through a centralised unit within the Ministry of Justice, which creates a bottleneck and often slows down procedures. They suggested devising alternative mechanisms that would allow specific key institutions to establish direct contact with their international counterparts (e.g., Public Prosecutor's Office, Labour Inspectorate, Ministry of the Interior).

The Norwegian authorities noted the need to enhance existing agreement and set up new agreements with the victims' countries of origin when the latter are outside the EU. This is a point also raised by the French authorities, which stressed that "a number of criminal organisations using ICT originate from countries with which international cooperation is either insufficient or non-existent. This is the case for the Chinese networks and the networks from Russia and Ukraine". Thanks to ICTs, these criminal networks can organise their operations in a way that allows the main members to control prostitution activities from their country of origin – often knowing that requests for judicial cooperation will not be fulfilled in a timely manner, if at all. Slow or lack of cooperation impact on the identification of offenders, collection of evidence and shutting down of Internet websites.

ZOOM | What can be learned from the EU judicial framework?

There is little doubt that the EU judicial framework offers a more integrated legal space able to smoothen judicial cooperation compared to the situation State Parties face when seeking cooperation outside such framework (albeit with limits and challenges). What elements of such framework could be extended beyond intra-EU cooperation? This is a difficult question that would require a comprehensive legal analysis, but we can sketch out here some preliminary suggestions. The submission by the Swiss authorities (i.e., a country outside the EU judicial framework) nicely summarises the key advantages of the EU framework, particularly of the European Investigation Order (EIO):

- it is based on a common set of rules with a wide scope of application;
- it sets clear deadlines for the collection of evidence;
- the grounds for refusal are limited;
- it reduces the administrative burden through the introduction of a uniform standard form;
- it ensures the protection of the essential rights of the defence.

It is clear that some measures can only be extended if they are part of a comprehensive set of shared legal rules. However, State Parties might wish to consider what specific aspects of the EIO can operate outside the EU framework. This could cover cooperation among the State Parties to the Council of Europe Convention of Action against Trafficking in Human Beings and the European Convention on Human Rights. Measures around setting deadlines for the collection of evidence and reducing the administrative burden through the introduction of standardised procedures could potentially be implemented without radical changes to domestic legal systems. Some enhanced, common set of rules could also be envisaged, provided that the provisions set out in the European Convention of Human Rights are upheld by a State.

Additional issues related to MLAs. The evidence submitted by State Parties also points to challenges in processing MLAs resulting from the lack of personnel adequately trained to compile and handle such requests – as well as the use of outdated technology. For instance, some countries have indicated that they do not always use secure e-mails and other forms of electronic correspondence when exchanging documents with foreign partners. Developing the use of secure forms of electronic communications, including rules and safeguards, and promoting their adoption among all State Parties might go some way to improve international cooperation among countries. Additionally, disseminating practical information about the contact points/dedicated units within a country that can serve as "privileged contact" in the case of THB cases, including ICT-facilitated THB, might also smoothen procedures.

2.3.2. Electronic evidence

While challenges related to obtaining electronic evidence are often linked to MLAs, the nature and relevance of such evidence pose a number of additional challenges that it is worth discussing separately.

As pointed out by the Austrian and British authorities, electronic evidence can make it difficult to identify the exact location of the data. Determining the country under whose jurisdiction the data fall might not always be straightforward – thus making the drafting of MLA requests challenging. The Portuguese authorities consider the system for obtaining electronic evidence from other countries as not 'fit-for-purpose', and it has been suggested that the 2nd Additional Protocol to the Budapest (Cybercrime) Convention[15] may offer improvements on the current system. Similarly, the Greek authorities have called for a common legal framework for the rapid exchange of digital evidence (noting that there is an existing common legal framework for the preservation of evidence).

An issue has been raised about the timing when a request for electronic evidence can be legally made. According to the British authorities, "sometimes law enforcement require access to the content of communication before they can demonstrate probable cause but the precondition for obtaining such assistance needs to be satisfied before the content is shared". This impacts particularly the early stages of an investigation. Similarly, the Austrian authorities pointed out the challenge constituted by the "high threshold for getting content-data from some jurisdictions". The same authorities have raised the issue of what type of information is possible to request during an investigation and on what legal basis (e.g., with or without a court order). The Austrian authorities have called for a "standardised access to CID information during THB investigations" (e.g. requesting subscriber information from mobile network operators). They pointed out that "in some countries [this is] only possible after the competent court has sent a European Investigation Order. In Austria, this is possible without a court order during CID investigations".

As already mentioned earlier in this report (Section 2.1.6), rules about the length of data retention are flagged up as particularly problematic. Several countries have expressed concern about the lack of a homogeneous regulation about data retention – thus hindering the

[15] Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe - News (coe.int)

exchange of electronic evidence. Some countries may not possess any data retention legislation.

Finally, several countries have expressed concerns about accessing electronic evidence held on computer servers located outside their jurisdiction. Experiences in this respect vary depending on the country and the company holding the data. However, there is ample evidence of difficulties in identifying a company, locating it, getting its cooperation and arranging for the transfer of evidence. State Parties have expressed the need for a more comprehensive framework regulating retention and transfer of electronic evidence, as well as a common legal framework replacing current ad-hoc bilateral working agreements between a State and a private company holding the data.

2.4. Challenges to cooperation with private companies

The study explored the challenges State Parties face when working with ICT companies and Internet service providers, including content hosts and social media, in tackling THB. While some of these challenges overlap with issues already discussed above, it is nonetheless beneficial to offer some further considerations on the issues highlighted by the State Parties. Below is a summary of such challenges:

- Obtaining a timely response from ISP companies and content hosts. Approaching hosts via rogatory letters sent through relevant authorities might entail long waits – with the risk of content being deleted by the time the request is acted upon. The French authorities have highlighted the long response time to requests for meta data related to accounts linked to offenders; for content data, there often needs to be an MLA request, which can take several months to be fulfilled as companies are often situated outside the jurisdiction of the requesting country (and the European Union).

- Clarifying the legal requirements under which ICT companies and providers of Internet services operate. The Austrian authorities have expressed concern that "international providers often impose formalistic, legally unjustified requirements on law enforcement agencies as preconditions for providing information and handing over user data and content. Enforcing prosecution orders is sometimes very complicated". According to the Belgian authorities, refusals are often not adequately motivated and explained. The authorities of Bosnia and Herzegovina have flagged up difficulties in getting non-personal data during investigations (before a court order can be issued). Identification of the ISP itself can create challenges – as pointed out by the Finnish authorities.

- The French authorities have highlighted issues related to the non-recognition of the prosecutor's office as an independent judicial authority when issuing a formal request for data requisition; a further issue is the requests from companies to disclose a large amount of evidence from an on-going investigation before a decision about handing over the data can be taken by the company's legal department.

- The Belgian authorities have noted the lack of feedback on operations internally carried out by companies, e.g. in relation to the removal of content. They also noted difficulties in communicating with companies –often compounded by frequent changes in contact personnel.

- As already noted, the lack of harmonised legislation around data retention and inadequate legal provisions are flagged up by countries as posing crucial challenges. In Norway, for instance, ISPs are not allowed to store information about IP addresses for more than 21 days, and they are not required to store information on the link between subscriber and IP address. According to the Norwegian authorities, this makes it "difficult for the police to identify suspects of ICT-facilitated THB". This issue is exacerbated when dealing with companies that are set up to provide anonymous and encrypted services.

- The Moldovan authorities have noted the lack of a designated contact point within private companies operating social media and other networking applications. It has been suggested that a contact point for each country/area (depending on the number of users) should be established. (One can also think of contact points designated based on the language spoken). Moldovan authorities have suggested making the establishment of contact points mandatory for ISPs, content hosts and social media. The issue of language skills within companies has been flagged up by the the Slovak authorities, who noted that large companies operating in multiple countries often lack staff possessing the language and legal skills relevant to every country they operate in.

- It is not always clear to ISPs which are the national agencies responsible for certain decisions, e.g. taking down illegal content. Slovak authorities suggested introducing the role of 'trusted flagger', i.e. identify specific agencies that are tasked with liaising with international providers to take down content and acting on other legal provisions. The trusted flagger would have an open communication channel with the companies and build mutual trust.

Several countries, including Cyprus, Ireland, Latvia, Luxembourg, Malta, the Netherlands, and the UK have indicated that ISPs, content hosts and social media companies have generally been cooperative when it comes to issues related to THB and child sexual exploitation. However, the British authorities have pointed out the need to go further and work with online companies "to **design out opportunities** for trafficking on their websites and work cooperatively with law enforcement to prevent trafficking occurring".

The Cypriot authorities referred to the use of Sirius – a platform to facilitate cross-border access to electronic evidence run by Europol – as an example of good practice. Such platform gives law enforcement agencies the ability to directly communicate with private companies for data preservation and disclosure. This was also highlighted by the French authorities (Project E-Evidence).

2.5. Evidence from NGOs

In addition to the evidence from State Parties, the study asked NGOs that provide assistance to victims to indicate the challenges they observe in the context of technology-facilitated THB.

2.5.1. Challenges to identification and investigation

Overall, the evidence from NGOs is in line with the challenges indicated by State Parties and discussed earlier in this chapter. More specifically, NGOs have highlighted the following set of factors hindering the detection of technology-facilitated THB and subsequent investigations:

- Lack of capacity among law enforcement, including lack of training, hardware and software, as well as limited use of special investigation techniques. Some NGOs have noted the lack of specialisation among the police and judiciary in relation to technology-related THB as well as a lack of capacity in the area of big data. Web-scraping tools trialled by Hope Now (Denmark) in 2016-2018, however, have achieved modest results.

- Fast-changing technological landscape, as well as offenders' *modus operandi*. Professionals can find it difficult to keep up to date with technology-facilitated THB, hindering their ability to promptly identify cases and launch investigations. Knowledge about the technical landscape and practices often sits in silos (e.g., law enforcement, private companies, NGOs, academia).

- Use of private forums, chat rooms or encrypted apps for contacts between offenders and victims. This makes it difficult to (a) detect such contacts and (b) acquire them as evidence to be used in court. NGOs have suggested including information/warnings on the safe use of private channels of communications.

- Difficulties in unmasking anonymous offenders during live streaming of online exploitation, as well as difficulties in gathering evidence of such abuses unless screenshots of video recordings are taken.

- Professionals find it challenging to ascertain whether a person behind an online profile/advertisement is voluntarily providing the services listed based on the information publicly available (e.g., in the case of online advertisements for sexual services). This is because offenders can create and manage online profiles on behalf of their victims. Furthermore, offenders can find it easy to re-create profiles when banned.

- Rules about data protection and privacy can hinder the identification of victims as well as traffickers. GDPR rules limit the use of technology to detect digital trails left behind by both victims and offenders (on social media, on the Internet but also in relation to financial accounts). There is a lack of comprehensive analysis of victim-centred digital trails including, for instance, real estate, bank accounts, ATM transactions, credit cards transactions, and medical records to facilitate investigations.

- Lack of interdisciplinary technology collaboration among private companies, public agencies and NGOs to fully exploit the increasing amount of data on THB. Sustainable Rescue Foundation has cited the following factors hindering cross-sector data collaborations:
    - independent hubs fail to attract law enforcement agencies or government;
    - lack of a technology strategy in THB national action plans;
    - law enforcement IT groups lacking the capacity or budget to develop, test, implement, train, update and maintain THB detection applications in a timely manner;
    - difficulties in sharing victims' data;
    - commercial interests.

- Limited THB investigations by financial institutions. Identification opportunities in Know Your Customer (KYC) data are not exploited due to lack of THB training and awareness as well as the complexities of the reporting system (quality of alerts, very large number of false positive, long response time, etc.).

- Lack of investments in Artificial Intelligence (AI) capabilities and the use of machine learning for operations, prediction and prevention. The Sustainable Rescue Foundation pointed to the use of machine learning in the medical sector as an example where "information is shared between clinics, hospitals, doctors and academia without infringing on privacy legislation. This is done using data visiting FAIR (Findable Accessible, Interoperable, Reusable) principles for metadata matches and Federated learning for deep analysis from multiple sources". They also noted that "no such investment or strategy is currently underway in THB organisations".

- Lack of data sharing between different entities at the local, regional, national or international level due to the lack of operational capabilities within law enforcement and limitations set by national legislations. Additionally, data are often collected in an un-structured form, which makes it difficult to share and further analyse the evidence.

- NGOs that provide direct support to THB victims, through online platforms, chat consultation and helplines, do not have the capacity, resources and technical tools to detect technology-facilitated online exploitation on a regular basis.

- Lack of awareness about risks and potential consequences linked to the use of technology among people at risk of trafficking. This is particularly acute among children and young adults. More generally, there is a lack of awareness among the general public about technology-facilitated THB, which results in low reporting.

2.5.2. Challenges to cooperation with law enforcement

All NGOs report some form of cooperation with law enforcement agencies, including signalling THB cases or providing assistance to victims following a request from authorities. Reflecting on their cooperation with law enforcement, NGOs have highlighted the following challenges:

- Conflicting goals or different approaches between NGOs and law enforcement, including decisions on whether a case should be further investigated.

- Issues related to data protection and privacy.

- Lack of feedback on cases that NGOs had flagged up to the authorities.

- Lack of resources to support cooperation between law enforcement and NGOs (this was pointed out also in relation to the innovative 'field labs' set up in the Netherlands, on which boards the Sustainable Rescue Foundation sits).

- When it comes to children, there is a lack of training among law enforcement on how to approach underage victims and persuade them to cooperate with the investigation. La Strada Moldova pointed out that investigations involving children have the added complexity of evidence management, as "children usually feel blamed, guilty, or ashamed of what happened to them, are not collaborative, do not want parents to find out about what happened to them or other people to see their sexually explicit video materials. Being afraid, many of them refuse to file a complaint", thus preventing further investigations by law enforcement agencies.

2.6. Tech companies

Facebook has indicated that content related to human trafficking is 'rarely reported' by users. They have further noted that underreporting might be due to a number of factors including: (a) trafficking victims might not have the freedom to report or might be unaware of their exploitation conditions; (b) buyers of services provided by a trafficked person might not be aware that they are purchasing a service from a THB victim or they are disincentivised to report "as they want to avail themselves of illicit or significantly cheaper services provided through exploitation". In other instances, it is noted that "for certain forms of human trafficking such as domestic servitude, since it may generally be a socially accepted phenomenon in some regions, bystanders do not realise they can or should report this content".

As for the challenges to cooperation with law enforcement, IBM has noted that there is "a number of obstacles"; primarily, they highlighted "concerns as to the legality of such cooperation, especially relating to data privacy concerns and the legal complexity of multiple jurisdictions". They called for "clarification on the international legal permissions for gathering and sharing data (with authorised law enforcement entities)". Facebook has indicated that the cross-border nature of human exploitation "presents challenges". For example, they noted, offenders might be based in a different country than the one where the victims are trafficked and abused: as such, "multiple jurisdictions may be involved in investigating a criminal network. Coordination among law enforcement within the EU and beyond adds additional complexities to anti-human trafficking efforts".

2.7. Further evidence from the landscape analysis

In addition to the evidence provided by State Parties, NGOs and tech companies, the study has also conducted a desk research of the available evidence base on the challenges related to detection, investigation and prosecution of online and technology-facilitated THB.

Of particular interest, it is the evidence related to challenges in the **identification of trafficking-related job advertisements**. It has been suggested that identifying advertisements rather than victims might be a good way to leverage technology: this goes back to the seminal works by CoE (2007) and Fine Tune Project (2011). The Fine Tune Project (2011) has offered a preliminary list of **red flags in the context of labour exploitation**. These include: (a) unrealistically high salary for unqualified jobs; (b) job descriptions lacking details, including no description of job role, location, place of work, and daily working hours; (c) no address for the company or agency hiring; and (d) no contact details apart from a phone number or a generic email. However, the evidence suggests that the identification of true positives (i.e., trafficking-related ads) remains very challenging. Several authors have pointed to the **difficulties in sorting** genuine advertisements from trafficking-related ones, despite the efforts put into developing **indicators of potential risk** (as well as re-interpreting the general UNODC and ILO indicators to adapt them to the online context: Di Nicola et al. 2017; Raets and Janssens 2018; Volodko et al. 2019):

a. In a set of 430 Lithuanian online job advertisements analysed by Volodko et al. (2019), 98.4% contained at least one indicator of human trafficking, thus suggesting that such indicators are often commonplace characteristics of low-skilled labour markets. Some hope,

however, comes from the finding that only 15% of advertisements presented more than five indicators, thus suggesting that with further refinement and appropriate analytical techniques, some harm-reduction strategies could be efficiently implemented.

b. Besides refining the available set of red flags (and constantly updating it, which poses an additional challenge), computational approaches based on web scraping, natural language processing, entity-recognitions and 'tags', and machine learning techniques more generally have been suggested as a potential way forward (Volodko et al. 2019 among others; also UN Delta 8.7). While potentially promising, this road opens up new challenges, including: (1) the need to establish a 'ground truth' for the models, which can only be done through close collaboration between law enforcement agencies and the private sector; (2) the need to leverage on private sector knowledge, as law enforcement agencies hardly have the required skills in-house; (3) the need to carefully assess the ethical issues related to large-scale machine learning techniques; and (4) the potential for discriminatory practices as well as issues of data protection and sharing information between different entities.

In some instances, advertisements for jobs in modelling, entertainment and – in some countries – sexual services abroad might be used to recruit individuals who are then coerced into sexual exploitation. A number of red flags has been suggested to separate trafficking-related advertisements from legitimate ones, including advertisements which: (a) are poorly written and unclear; (b) are overpromising; (c) are too broad; (d) do not specify the destination country (providing a reference to 'exotic destinations'); and (e) do not contain the full name of a contact person, a recruitment agency and/or a company that would employ the successful candidate (Di Nicola et al. 2017). However, preliminary attempts to screen openly available evidence using these criteria have pointed, once again, to the difficulties in separating trafficking-related advertisements from false positives.

Detecting instances of sexual exploitation on the basis of **online advertisement for sexual services** is equally challenging, i.e. sorting sexual services provided by trafficked persons from those voluntarily provided by individuals based uniquely the text and visuals included in the advertisement. Some indicators of exploitation have been suggested, including discrepancies among profile descriptions, pictures and locations; such discrepancies can also be cross-checked across multiple websites (Di Nicola et al. 2017). Phone numbers have been shown to play a key role, for instance in detecting the presence of the same phone number in advertisements, websites and posts attributed to different persons (a potential red flag). It has been suggested that facial recognition can be deployed as a technique to spot inconsistencies and red flags, similar to the approach adopted in detected sexual materials depicting minors (Raets and Janssens 2018).

However, preliminary attempts to scale up the above detection strategy have shown clear challenges. In their attempts to identify victims of sex trafficking in the US through online escort advertisings, Ibanez and Ganzan (2014, 2016a and 2016b) used phone numbers and indicators of movement, but failed to produce strong results. Additionally, some of the indicators listed in Ibanez and Gazan 2014 are rather puzzling and might not be indicative of human trafficking at all; in some cases, they might even point to the opposite situation.

3. Strategies and good practices

Having discussed the challenges, the study now turns to explore the strategies that State Parties have developed to detect and investigate online and technology-facilitated THB, to foster international cooperation and to identify and assist victims. This is then followed by a discussion of the evidence provided by NGOs and tech companies on the same issues.

3.1. Detection of ICT-facilitated THB cases

3.1.1. General strategies

Countries have indicated pursuing a variety of strategies to detect online and ICT-facilitated cases of THB. A widely cited strategy is **Internet monitoring**, including forums and, in some cases, TOR networks (Dark Web). This is often combined with the use of **Open-Source Intelligence (OSINT)**, that is a very common investigative strategy that consists in collecting data from social media and other publicly available online sources about a person's network of contacts, living conditions and financial situation. OSINT can be used 'proactively' e.g., to detect potential THB cases, to identify potential offenders and victims or to obtain fresh information. Some countries have formed **'cyber-patrols' with specialised officers** tasked with carrying out OSINT investigations on the Internet. Some jurisdictions allow for covert online investigations (cyber-infiltration). In the Netherlands, specialised investigators with **'digital knowledge'** can be employed in THB investigations to collect online evidence of THB. The Finnish authorities have noted the recent establishment of a sub-unit to tackle online THB within the National Investigation Team (they also reported the presence of an Online Intelligence branch operating on the web, including the Dark Web).

Linked to OSINT investigations, countries have cited the use of **social network analysis techniques** to understand and reconstruct the network of contacts of an offender and/or victim. To give an example, if victim A is linked to recruiter B, one can then assess all the contacts of recruiter B to identify potential victims. **Relational information** is key and it is increasingly leveraged by police forces through the so-called 'link analysis' or more sophisticated 'social network analysis' techniques.

Additional **proactive strategies** include the use of technological tools to search for online evidence (e.g., web-crawlers, see also below) and strategic investigations into the ICT *modus operandi* of THB offenders. Generating – and updating – such strategic (broader) knowledge of the phenomenon can inform a holistic approach as well as specific, more targeted, investigations. Not all State Parties, however, have indicated using 'strategies'. A few State Parties have expressly indicated that their investigations into ICT-facilitated THB remain 'reactive'.

Authorities have reported establishing direct contact with online service providers to identify ICT-facilitated cases of THB. In countries where advertising online sexual services is legal, authorities may "perform targeting filtering of phone numbers and [analysis] of user data associated with [presumed] offenders" (submission from Hungary). A Cantonal Police Force in Switzerland carries out 'targeted checks' of online advertisements of sexual services in order

to detect potential victims of THB. **Web-scraping tools** specifically developed for extracting information from websites are employed by some law enforcement agencies in the UK to identify risks and vulnerabilities on Adult Services' Websites (ASWs). The British Police forces undertake web trawls of ASWs to gather data which is then used to analyse activity on ASWs and potentially turn these data into actionable intelligence.

Several countries have mentioned the availably of a **mechanism for Internet users to report content and websites** they suspect to be linked to illegal activities, including sexual and labour exploitation (see below for some examples).

3.1.2. Country-specific strategies

To further explore the various strategies developed by countries to tackle and counteract the misuse of the Web, including online job advertisements, in the context of technology-facilitated THB, we now offer a brief review of country-specific mechanisms and initiatives. Such strategies should be read together with the good practices discussed in the next section as well as the discussion on domestic legal frameworks related to the identification and removal of online THB-related content included in the Web Appendix.

In Albania, there is a **mechanism of permits** associated to online job advertisements, and these are issued/controlled by institutions (unspecified in the submission).

The Austrian authorities have intensified proactive searches on various online platforms since the outbreak of Covid-19 to identify THB victims and offenders leveraging on **special software technologies** (e.g. web crawlers), **officers specialised in Open Source Intelligence** (OSINT) as well as **undercover agents** (online undercover investigations). Activities are carried out jointly by THB investigators and officers specialised in IT. It is believed that this model might offer a template for future investigations.

The Belgian authorities have indicated that the current 'abolitionist model' adopted in relation to prostitution make it legally impossible to conclude agreements with websites publishing advertisements for sexual services. This is seen as a 'limitation' of the current legislation. The NGO "Child focus" is currently developing an awareness campaign for clients using websites hosting advertisements for sexual services to inform them of the risk of coming across an underage person. This campaign is being carried out in partnership with the websites concerned.

The Croatian authorities have reported conducing **checks on social networks profiles** of individuals connected to specific criminal investigations, e.g. sexual abuse and child sexual exploitation, to identify potential victims and recruiters. Such checks are carried out by specialised cybercrime officers.

In Cyprus, there are awareness-raising campaigns organised by the Cybercrime Department (CCD) aimed at schoolchildren and their parents as part the National Strategy for a Better Internet for Children. Since 2014, the CCD also runs a reporting platform for cybercrime (www.cyberalert.cy).

In Estonia, members of the public can contact '**web-constables**' to report social media content potentially linked to illegal activities, including THB.

French law allows investigators to **cyber-infiltrate criminal networks**. Law enforcement agencies employ investigators to cyber-patrolling the web to **detect advertisements** and **identify criminal networks**. Targeted surveillance operations on specific Internet forums are also carried out, using covert investigation techniques where necessary. Investigators also use Internet advertisements to cross-check geographical data collected via other sources to identify places used for THB. Information collected from different sources is systematised and used to **reconstruct criminal networks, i.e. relations among places, offenders and victims**. In addition, French law enforcement agencies are working towards setting up **cooperation protocols** with social network companies and online private rental platforms to foster provision of information. As online content hosts may in some cases be overwhelmed by the volume of requests for transmission of information and evidence requisitions, the authorities suggested **devising more direct – and simplified – procedures underpinning cooperation** between content hosts and law enforcement. For example, 'Wannonce', a French site used for advertisements linked to underage prostitution, sends to law enforcement a link allowing a direct search within their database upon provision of an email address. Finally, Article 6(I)(7) of Law No 2004-575 of 21 June 2004 on "Trust in the Digital Economy" (LCEN) requires Internet access providers and website hosts to assist in combating the dissemination of materials related to specific offences, including THB. They are required to set up an easily accessible and visible mechanism enabling any person to **flag suspicious material**. Companies are also obliged to promptly inform public authorities of any illicit activities that are reported to them and carried out by recipients of their services. Members of the public can report illegal content on the Internet to the police and Gendarmerie via a website (www.internet-signalement.gouv.fr). Reported content is examined by PHAROS (*Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements*), which is a specialised police unit.

In Finland, the Child Protection and Finnish Hotline (*Nettivihje*) offers a way to report online child sexual abuse material and child trafficking. *Nettivihje* works closely with the National Bureau of Investigation and their team specialised in sexual crimes. The Finnish Police also has an online tip-off to report suspicious activity on the Internet including materials potentially related to sexual offences against children. This template can potentially be expanded beyond child sexual exploitation.

In Germany, police have started (May 2020) to use an **automatic searching tool** to analyse a large amount of data published on adult advertisements' websites. The searching tool structures the data in order to assist with the extraction of relevant information. This is done in conjunction with the use of specific indicators. The authorities consider the use of this automated tool as 'very helpful.

The Greek authorities have mentioned the **monitoring of websites and forums advertising job posts** or services to detect online THB-cases. This is done through a close cooperation between the Anti-Trafficking Units of the Hellenic Police and the Cyber Crime Division. In addition, the Cyber Crime Division of the Hellenic Police has developed awareness-raising and educational activities focusing on the responsible use of new technologies and online risks, for example, the "Safe Surfing Day Seminars" and the "Cyberkid" website and app, informing students, parents and teachers on violence on the Internet and the risks they

might face on social network websites. The NGO 'Smile of the Child' holds regular events on Safe Internet Day (9 February).

In Iceland, the Reykjavik Metropolitan Police holds so-called '**Internet-weeks**', during which they sift through popular websites advertising sexual services looking for instances of THB. In case of suspicious activities, the police will ask for a court order to wiretap the telephone numbers listed in the adverts and launch investigations.

In Ireland, the Human Trafficking Unit Coordination and Investigation Unit of An Garda Síochána (the Irish Police) liaises with various social media and recruitment companies in order to raise awareness of potential THB-related recruitment posts. Irish-based and some international ICT companies are normally cooperative when An Garda Síochána request to remove online content that is judged as illegal.

In Latvia, there is an official website for job advertisements run by the State Employment Agency. The website seeks to prevent instances of labour exploitation by **offering a safe advertisement space.**

In the Republic of Moldova, there are currently no specific automatised mechanisms to identify advertisements and online content potentially linked to THB, and the authorities are currently working with the Netherlands to acquire the web crawler developed by the Dutch law enforcement.

In the Netherlands, the **police can set up online fake profiles** (*lokprofiel*) to identify – and then investigate – THB cases and offenders. Additionally, the Ministry of Justice and Security is currently exploring the role of technology in all phases of THB through expert meetings and research carried out in cooperation with the Centre against child exploitation and THB (CKM).

In Norway, the Cybercrime Centre is currently developing a **database of online sexual advertisements** published on a local website. Such information will provide the basis for further analysis.

In Slovenia, a Safer Internet Centre has been established in 2005 to raise awareness and help with the detection of illegal online content. It offers three main services: (a) an **awareness centre** on responsible use of Internet and new technologies (Safe.si) aimed at providing children, teenagers, parents, teachers and social workers with online/offline activities, education, workshops, content, awareness raising campaigns; (b) a helpline service for children, youths and parents (also known as 'Tom Telephone') with professional counsellors offering advice on safety on the Internet also via an **online chat room**; (c) anonymous online reporting of illegal online content.

In Spain, the authorities employ **social media tracing** by cyber patrols focused on detection of THB victims. These are carried out by the Guardia Civil Central Investigation Unit specialised in human trafficking and they have been intensified during the Covid pandemic. The Policía National has also recently created an investigative group specialised in THB cases on the Internet (Operative Group VI of Cyber-trafficking with the Central Brigade of Human Trafficking of Policía Nacional).

In Sweden, **regular surveillance of websites** advertising prostitution activities is carried out by the police to identify place and time of such activities (under Swedish law, all purchases of sexual services are illegal).

In Switzerland, some cantonal police forces use **covert investigations to check advertisements** on adult websites, as well as the individuals involved to uncover THB cases.

In the UK, the Gangmasters and Labour Abuse Authority alongside Crimestoppers used Facebook to inform jobseekers about fake recruitment advertising on social media. The team **created Facebook recruitment advertisements** that provided a hyperlink to a Crimestoppers' webpage, which in turn provided information on indicators of risk when seeking employment in the construction industry. The campaign targeted Romanian men aged 18-34 and reached over 900,000 people. There was a 13% increase in reports relating to THB and a 400% increase in THB reports relating to Romanian victims. As part of a multi-agency approach (Project AIDANT) bringing together National Crime Agency, Border Force, Immigration Enforcement, Her Majesty's Revenue and Customs, the Gangmasters and Labour Abuse Authority, and police forces, the authorities are **designing and testing new methodologies for industry reporting**. The NCA Modern Slavery Human Trafficking Unit (MSHTU) is working to raise standards on Adult Services' Websites (ASWs) by improving the way companies identify THB and exploitation on their platforms, and report it to law enforcement. Police Forces also utilise automated, open- source research procedures to collect information from advertisements on Adult Services' Websites (ASWs). The view taken by the British authorities is that closing down ASWs is risky, as it is likely not to lead to an elimination of demand resulting instead in the displacement of advertising onto other platforms to the detriment of both THB victims' and sex workers' welfare. Additionally, the Farm Work Welfare app has been developed with the aim of reaching seasonal workers and employers within the farming and food production sectors and a workers' voice scheme (SAFERjobs, www.safer-jobs.com) has been set up to enable transparent supply chains and gather intelligence on abuses in the labour market. Organisations found to be non-compliant get both enforcement action and messages to their end-hirer to raise the latter's awareness, potentially resulting in a loss of business (a 'name-and-shame' strategy).

In Ukraine, the authorities have started to block online channels on Telegram that disseminate information on sexual exploitation.

3.2. Investigation into ICT-facilitated THB cases

This section explores the strategies and good practices devised by State Parties to increase the effectiveness of investigations into ICT-facilitated THB (such strategies and good practices should be read in conjunction with the strategies related to the identification of cases discussed above as identification and investigation can be closely linked).

Several countries have highlighted the importance of providing law enforcement officers with **continuous training and development activities based on local and global best practices**. Setting up and training specialised units for ICT-facilitated THB have been mentioned as an important strategy. More generally, **investing in human capital** is seen by many State Parties as crucial as investing in technological equipment. Among the specialised profiles that countries have identified as key to effectively investigate ICT-facilitated THB, there are officers specialised in "new technologies", "operational criminal analyst", "undercover investigations" and "open-source investigators – OSINT" (the labels are those indicated in the French submission, but other countries have pointed to similar profiles).

As noted by the Greek authorities, training should be provided not only on how to use tech tools, but also on "their ethical use with respect of human rights and data protection" (more on training is in the next Chapter).

How training is currently conducted varies from country to country. One model is to entrust national Cybercrime centres, where established, with the task of developing tools and techniques, and the knowledge around them, and then *disseminate* this knowledge among police units and/or offering assistance by integrating other specialised unit, e.g. THB units. It is clear that knowledge about "advanced computer technology investigations and analysis, including trace and evidence security from digital devices, ICT systems, Internet providers" is a crucial asset (Norwegian submission). Several countries (but not all) have indicated that they possess a dedicated unit dealing with crime with a large technological component, e.g., Cybercrime Units/Centres or High-tech Crime Units. Other police units, e.g. specialised THB units, might request assistance from such units.

Several countries have noted the importance of including in THB investigations specialised investigative officers with '**digital knowledge**'. Such officers can be employed to search for online clues of THB. One operational model suggested by the French authorities would see the presence of personnel specifically trained in conducting investigations on the Internet and social networks embedded within each unit specialised in the fight against THB. Crucially, this personnel could be made of sworn police officers or non-sworn police officers, e.g. by creating technical support groups for 'traditional' investigators. This idea **moves away from the traditional police model** based on sworn police officers and adopts the principle – already followed by some police forces – of having non-sworn officers in more technical roles (e.g., analysts).

Besides providing training to officers, the Bulgarian authorities have highlighted the importance of engaging IT experts in THB investigations, as well as enhanced cooperation with the private sector. This is echoed by the Cypriot authorities who have indicated, as a potential good practice, the creation of teams of investigators and analysts specialised in THB and cybercrime. The value of **inter-agency investigative work** with the involvement and cooperation of a wide range of specialised staff was also highlighted in the submission by Switzerland where, for example, joint teams have been set up and this model could be extended to ICT-facilitated THB.

The German authorities have pointed to the importance of improving **knowledge sharing** among institutions and **strengthening ICT skills** among police officers. According to the Spanish authorities, it is crucial to both "increase awareness of Internet crime" and "include technology crime specialists from the outset" of THB investigations. A few countries have indicated that training on how to oversee and coordinate THB investigations with large technological component should also be provided and/or strengthened among prosecutors, as electronic evidence is becoming more and more substantial in THB cases.

There is fairly widespread consensus on the **importance of acquiring and having access to specialised software** to enhance investigations into ICT-facilitated THB. In the Netherlands, the authorities have created a web-crawling tool to collect and systematise large volumes of data. At the moment, Dutch law enforcement is trialling the tool on concrete THB cases to build up a judicial framework. According to the Dutch authorities, the web-crawler

"focuses on ads with a risk of sexual exploitation and is currently being tested"; the authorities are also working on determining if "there is sufficient legal basis and practical usability for its use in formal investigations".

Similarly, the **importance of big data, as well as improving big data capabilities**, has been highlighted by several other countries, including Estonia, Republic of Moldova and Greece. Developing or acquiring tools that are able to download webpages and other types of electronic information automatically is seen as crucial in conducting investigations. For example, in 2020 the Lithuanian Criminal Police Bureau acquired a licence for a software to collect information from online sources and a licence for a specialised software to analyse such information. However, it is not just the ability to collect data that matters. Crucially, such tools also need to be able to **store** such **information in a secure way** so that they can be *confidently* used "as evidence in court or as intelligence information in order to build a case" (submission by Sweden).

Two other types of tools are seen as crucial to conduct effective investigations into ICT-facilitated THB. First, tools for downloading information from mobile phones when the passcode is not available (submission by Sweden). Secondly, the development and introduction of tools that allow decryption of conversations over apps for personal communication. The Swedish authorities have pointed out that such tools should also be able to decrypt conversations in real time. In Austria, the Criminal Intelligence Service is developing a specific software for the examination of mobile phones to identify victims of THB.

The Swiss authorities have highlighted the need to increase **undercover investigations** – hence investing in the training of specialised officers. Similarly, they highlighted the importance of specially trained police officers in the field of THB. Covert investigations are regarded by the Norwegian authorities as "the most efficient investigations", specifically when combined with the collection of big data from OSINT web searches as well as money transfers/flows. In the Netherlands, police are currently testing the use of "catfish profiles" to identify traffickers during their attempt to recruit potential victims. Similarly, the Spanish authorities have flagged up the need to adapt domestic legislation to fully exploit the possibilities afforded by undercover online investigations.

The British authorities estimate that the **layering of information** is critical to investigate ICT-facilitated THB. Enriching intelligence pictures via the combination of open source and law enforcement system research is deemed as good practice. They also suggested moving away from simple lists of indicators. For instance, they noted that in the context of sexual exploitation, investigators normally follow a three-step process, as opposed to a prescriptive list of indicators, to identify high risk ASW advertisements. According to such process, risk is identified where ASW advertisements are part of a network, where indicators of coercion and control are present and where the authenticity of the advertising account is suspicious.

Several countries have noted the importance of enhancing cross-border cooperation and ensuring a prompt data exchange at the operational level. The Austrian authorities have indicated the **mutual exchange of officers** with the victims' countries of origin as an example of good practice. More generally, strengthened international cooperation with investigative authorities in the countries of origin is seen as good practice.

The Finnish authorities have highlighted the importance of carrying out **strategic analysis** to generate knowledge on emerging trends and up-to-date information on offenders' *modus operandi* (including technology and websites used by offenders). This view is supported by the Polish authorities. It is recognised that constant monitoring of the phenomenon is a difficult and time-consuming activity, adding to the (often) already stretched police resources. However, having access to an up-to-date knowledge base, including recruitment techniques used by perpetrators, is seen as a very effective tool to prevent and combat THB. This knowledge-gathering exercise should have an international dimension – ideally with some degree of international coordination. Based on this shared evidence, individual countries can then launch targeted police operations and set up cooperation agreements whenever relevant.

Several countries have noted that investigations could be facilitated by an **easier cross-national preservation of evidence and its access**. This potentially translates into facilitated and streamlined procedures for dealing with inquiries sent to units responsible for data preservation in foreign countries (data preservation requests), as well as in the facilitation of requests for mutual legal assistance. As pointed out by the Polish authorities, among others, it is "the private sector that is most often in possession of information of interest to law enforcement authorities (e.g., subscriber data)" and an "effective and fast acquisition of such data by the police is important for a positive solution of an investigation".

3.3. Fostering international cooperation

Reflecting on their experience in handling cross-border ICT-facilitated THB cases, countries have identified the following 'good principles' to foster international cooperation:

- Leveraging on resources available within agencies such as Europol and Eurojust, as well as setting Joint Investigation Teams.
- Establishing contact with other parties at the **early stage** of an investigation. This calls for organisational measures facilitating such swift interactions (e.g., through clarity around procedures and clear contact points).
- Developing a very good **understanding of legal context and opportunities** for cooperation with the country or countries concerned to avoid blocks and ensure a timely collaboration.
- Creating **coordination meetings** to exchange information and evidence as swiftly and quickly as possible, to lay out a common strategy from the *outset*; to facilitate the execution of international legal aid requests and to remove obstacles related to the admissibility of evidence in a given country.
- Developing a **common understanding** of standardised approaches and ensuring **transnational interoperability** of law enforcement agencies through transnational training sessions.

Besides these general principles, there are also a number of specific examples of good practices identified by State Parties. Such practices can be grouped in the six main categories below.

Joint Investigation Teams. An example of good practice in international legal cooperation reported by the Bulgarian authorities is the Joint Investigation Team set up in 2019 with

France – and the assistance of Eurojust – targeting trafficking in human beings, child sexual abuse and trafficking in pregnant women for the sale of their children. A large number of investigation activities were conducted by the JIT in Bulgaria, France, Germany and Greece. More generally, several submissions have indicated Joint Investigations Teams as an example of good practice. As explained by the Austrian authorities, they allow for a "less bureaucratic exchange of information when it comes to transnational investigations, as well as a division of competencies between participating judicial authorities".

Cooperation between labour inspectorates. The Bulgarian General Labour Inspectorate Executive Agency highlighted the importance of coordinated inspections and investigations jointly carried out across countries on complex cross-border cases involving potential labour exploitation among seconded workers[16]. The joint actions implemented between the labour inspectorates of Bulgaria and France (project *Eurodétachement*) are seen as an example of good practice. Actions included joint inspections of temporary employment companies sending workers to France, as well as information meetings for Bulgarian workers seconded abroad or directly employed in France (mostly in agriculture). Online meetings to exchange information and good practice on cross-border inspections were also held. This example is particularly interesting as it shows the **importance of non-police cooperation** – as much as police cooperation – in tackling THB. Yet, such cooperation tends to receive more limited attention in policy briefs. State Parties might wish to consider ways to improve cooperation among authorities other than police – particularly in the context of THB for labour exploitation.

Strategic Cooperation. The German authorities have highlighted the importance of strategic cooperation, for instance via the OA 7.1 of the Europol-based EMPACT project (*European Multidisciplinary Platform Against Criminal Threats*). This project focuses on online THB. As an EMPACT project, the Netherlands and the UK are developing a Visual Landscape on ICT-facilitators of THB.

EU/Internationally Coordinated Cyber Patrol Actions. The Dutch authorities and the Portuguese authorities have indicated the EMPACT Joint Action Days/coordinated cyber patrol actions on the Internet/Darknet as an example of good practice in international cooperation. Intelligence is first collected in individual countries and then coordinated actions are launched.

Leveraging on the network of liaison officers. The Polish and French authorities have highlighted the importance of accredited liaison officers to facilitate information exchange. The French authorities pointed to a case in which the support received from the Romanian liaison officers based in France made it possible to simultaneously carry out arrests in both countries. In this way, authorities were able to target the entire transnational criminal network, including its head who was directing operations in France while living in Romania. Norwegian authorities highlighted the benefit of having a contact point in the Philippines to share information about ongoing cases, thus avoiding duplications in investigations and conflicts. Through the contact point, Norwegian and Philippine authorities were able to share experiences, trends and studies, including on online-facilitated THB.

[16] As per Directive 96/71/EC and the Internal Market Information System (IMI).

3.4. Victims identification and assistance

This section focuses on the ways technological tools are leveraged by State Parties in relation to: (a) identification of victims; (b) assistance and (c) dissemination of information among at-risk communities.

3.4.1. Technological tools to identify victims of THB

The use of technological tools based on **facial recognition** appear to be widely used in the case of Child Sexual Exploitation (CSE), e.g. to cross-check images against existing international databases such as the NCMEC database (National Centre for Missing and Exploited Children, US) or the Interpol ICSE[17]. However, the use of such tools appears to be more limited outside CSE. Finnish authorities have indicated that they are conducting tests on facial recognition tools to identify victims of online sexual exploitation, particularly in the context of webcams. They have also suggested that the use of such tools could be broadened to encompass a wider range of THB situations. The Latvian authorities have mentioned the use of specialised software for image recognition (PhotoDNA, Clear View) on a case-by-case basis. In Hungary, targeted use of facial recognition tools may be employed during an investigation to identify potential victims. Among a few countries that have indicated using tech tools to identify victims of THB using big data, Germany has recently introduced a tool to scan websites featuring advertisements for sexual services to help identify victims of THB. Austrian investigators have access to **web crawlers** and (under specific conditions) facial recognition tools. In the UK, the authorities use web scrapping tools to collect and analyse data from Adult Services Websites (ASWs) to assist with the identification of THB victims.

Regarding the use of **THB indicators** ("**red flags**"), several countries have stated that they *do* rely on indicators for the identification of THB cases; however, these are 'general' THB indicators and not specific to ICT-facilitated THB. This is not surprising, as the development of indicators ("red flags") specific to ICT-facilitated THB is far from straightforward – as discussed at length in Chapter 2. The Norwegian authorities stated that, while they "do have a set of indicators to identify victims of THB", this needs to be revised and broadened to make it suitable to "the ICT-crime investigation environment". This work is currently being undertaken by the Norwegian National Expert Group on THB.

The British authorities have reported using a list of indicators to assist with the **identification of victims on ASWs**. Their experience on using such indicators together with a web scraping tool is particularly telling. According to the evidence submitted, while these indicators can provide some assistance, they "need to be used in conjunction with network analysis and assessments of account authenticity to ensure best practice". This is points to the difficulties in automatizing the identification of victims – and the limits of over-relying on a pre-set list of indicators. Moreover, the British experience shows the importance of combining different methods, including **social network analysis** and the **human assessment** of evidence. Once again, the key role of analysts/investigators emerges clearly – and so does the need to effectively train them. Tools can be very valuable in performing data reduction and handling

[17] Among the tech tools used by countries in the fight against child sexual exploitation (CSE), there are 'Gridcop' and 'IcacCops'. The Icelandic police use 'Griffeye' to process, sort and analyse images and videos seized during CSE investigations, and cross-check these images against international databases.

large volume of information; however, they need to be employed by well-trained operators with knowledge of the specific topic/issue (e.g., THB).

Using artificial intelligence and tech tools to identify victims is not without challenges, including **ethical issues** and potential for discrimination (e.g., profiling based on discriminatory criteria; see also the discussion in Chapter 6). Concerns has been expressed by the Swedish Police Authority in relation to "the use of AI technology to identify victims of human trafficking".

Finally, the Office of the Greek National Rapporteur and the Rights Lab of the University of Nottingham are piloting a project using satellite data and remote-sensing methods to monitor working conditions and mobility of migrant workers in agriculture. The Greek Rapporteur is in the process of developing further technological apps for the identification of THB victims in the agricultural sector and has made the development of new tech apps a key component of the National Action Plan 2019-2023.

3.4.2. Technology-based initiatives to assist victims and disseminate information to at-risk communities

This section presents an overview of technology-based initiatives devised to assist victims and disseminate information to at-risk communities. Please note that the initiatives discussed below have been identified by the State Parties.

Online Reporting Mechanisms and Helplines. Several countries have mechanisms in place to anonymously report victimisation, as well as receive initial assistance through helplines. Some helplines offer 24-hour support and can direct victims to social services, explaining procedures and rights. In the Netherlands several organisations offer **digital assistance through a chat functio**n ('Fier' and 'Slachtofferhulp Nederland' are two of those organisations). Such organisations offer initial advice, assistance and the possibility to anonymously report sexual exploitation. The chat function is not only reactive, but also serves to proactively establish contact with individuals at risk. The Dutch Ministry of Justice and Security is currently investigating how this tool can be further developed in collaboration with relevant stakeholders. In France, the Ministry of the Interior runs a platform for reporting sexual and gender-based violence (PVSS). Victims can get in contact with an official via **instant messaging/online chat**, make a report and receive first assistance.

Online Official Materials. Informative materials produced by authorities are often posted on official websites. In Austria, for instance, information for THB victims produced by the Federal Ministry of the Interior, as well as by NGOs, is available in several languages on various online platforms and social media. On the website of the Federal Ministry of Justice, victims of THB can access materials in 16 languages on their rights to psycho-social and legal support. In Poland, the Ministry of Interior and Administration and the Ministry of Foreign Affairs ran an online information campaign through the 'e-konsulat' website with a banner displaying information on THB in several languages and redirecting online visitors to the Consulting and Intervention Centre for the Victims of Trafficking (KCIK). Besides official channels, several countries have highlighted the important role played by NGOs in disseminating information through their own websites, as well as their official accounts on social media such as Facebook, Instagram and YouTube.

Online Tools and Apps. The Bulgarian National Commission for Combating Trafficking in Human Beings launched an online prevention tool as part of the annual campaign for prevention of THB for labour exploitation. The online tool was created in cooperation with a Czech NGO and was targeted to Bulgarians looking for a job in the Czech Republic. The tool provided information on labour conditions and risks of worker rights' violations. As noted by the Bulgarian Commission, "the effectiveness of this approach was highlighted by the fact that shortly after the tool began functioning, a fake one was created aiming to attract potential victims of labour exploitation". In Lithuania, an app called 'Raktas' (available on Google Play) has been recently developed to raise awareness among Lithuanians living and working abroad about early signs of THB. As a future development, the app will include a chat facility through which a Lithuanian victim or presumed victim of THB will be able to contact a Lithuanian NGO in real time and request support. The Portuguese Labour Conditions Authority has developed the App 'ACT', Agir Contra o Tráfico. The Estonian authorities report the use of mass notification via SMS/text messages as part of a campaign against sexual exploitation. In 2017, Spain launched the mobile app "Chicas Nuevas 24 horas: Happy" to let young people discover, through a video game, the journey of a girl (Happy) from her hometown in Nigeria to her experience of sexual exploitation in Spain.

Online Awareness-raising Campaigns. In Bulgaria, the National Commission for Combating Trafficking in Human Beings (NCCTHB) conducts three nation-wide prevention and information campaigns each year with a series of events focussing on prevention of trafficking both for forced labour and for sexual exploitation. Materials are also distributed online. Over two million Bulgarian active users were reached on Facebook and Instagram during the October/November 2018 campaign. More generally, NCCTHB activities and related online prevention tools are published regularly on social media. Such posts reach approximately 100,000 users/year. Additionally, discussions on ICTs, Internet, social media and the impact of new technologies on THB, as well as their use for recruitment and exploitation of victims, are included in different awareness-raising activities at national and local level, targeting young people and students. The General Labour Inspectorate Executive Agency organises and participates in information campaigns on the risks related to working abroad; it also runs a telephone line for advice and reporting also open to Bulgarian citizens working abroad.

In Ireland, the ongoing Blue Blindfold campaign run by the Department of Justice regularly disseminates information to at-risk communities through a dedicated website, print media and social media campaigns.

In Germany, the Federal Ministry for Economic Cooperation and Development has developed projects with partner countries to prevent and combat THB. For example, as part of the "Preventing Human Trafficking in the Western Balkans and Supporting Victims" project, the Migration, Asylum, Refugees Regional Initiative (MARRI) has created guidance notes and information materials for public awareness campaigns and made them available online. Since the Internet is increasingly being used to recruit victims of THB, one of the toolboxes focused on the threats that children are exposed while navigating online[18].

In Romania, the National Agency Against Trafficking in Persons (NAATIP) runs campaigns on Facebook, YouTube and, since 2020, also Instagram, Twitter and LinkedIn. Facebook posts

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

have registered an impact of 2.5 million users in 2020 (+300% over the previous year). Examples of campaigns include:

(a) Daily posting on social networks of anti-trafficking preventive messages on different types of exploitation (sexual exploitation, labour exploitation and forced begging);

(b) The online campaign "The perfect Job – one way illusion" in partnership with OLX Romania (a web service hosting announcements) aimed at preventing human trafficking through increased awareness among people seeking employment through online platforms;

(c) Enlisting two well-known Romanian YouTube vloggers with a combined audience of 1.3m followers to increase visibility and effectiveness of the NAATIP anti-trafficking messages. The vloggers recorded two videos on THB, which achieved around 100,000 views on You Tube in the first hours of streaming.

In sum, it is important to note that, as pointed out by the Bulgarian authorities, an effective campaign requires "a lot of preparatory work" to fully understand its target and adequately develop its message. Ultimately, this requires investment. A good practice is to work with private companies to produce **social advertising**. This can be done, for example, through publications sponsored by social media channels such as Facebook and Instagram (the platform could provide free space, as well as expertise in designing a campaign/message). Clearly, targeted and well-developed online campaigns can be a helpful tool. The example of a campaign ran by the Bulgarian National Commission for Combating Trafficking in Human Beings is telling. As part of the campaign – designed to raise awareness on THB for labour exploitation – a visual portraying an example of a deceptive job offer was produced and circulated. Users mistook the job offer for a genuine one and started to call the office of the National Commission, making inquiries about the job (see Section 1.1.2 for more details on the campaign). This example shows the potential reach/impact of deceptive job advertisements, but also offered the Commission "a good opportunity to inform jobseekers ready to accept risky offers".

However, as cautioned by the Bulgarian authorities, there is a **risk of over-relying on online campaigns** when trying to reach out to potential victims. In some cases, such victims come from "vulnerable communities" characterised by low education and limited familiarity with technological tools and resources. In those circumstances, outreach based on a direct (personal) approach (still) has an important role to play as a preventative strategy.

Finally, inspiration for initiatives can come from projects tackling issues similar to online and technology-facilitated THB. In Finland, for instance, the NGO Women's Line has launched a project called *Turv@verkko*, which aims to prevent cyber violence against women and girls, and assisting victims. Similarly, Youth Exit and *Sua varten* target young Internet users to prevent online sexual harassment. While not directly related to THB, such initiatives might offer useful cues to develop projects targeted to THB victims.

3.5. Evidence from NGOs

NGOs have reported a number of strategies to improve detection assistance of victims and awareness-raising in relation to online and technology-facilitated THB.

La Strada International, KOK (Germany), Astrée (Switzerland) and La Strada Moldova have stressed the importance of **adequate and up-to-date information** easily accessible online by trafficked persons and individuals vulnerable to exploitation and abuse. This should include information about support organisations and their helplines. Such online platforms should also **allow for the self-identification** of victims. La Strada International pointed out that relevant information acquired by NGOs should be shared with law enforcement – once consent of those concerned is acquired. Initiatives to increase self-reporting have been envisaged also in relation to labour exploitation, e.g. in the form of online platforms and apps through which people can anonymously report onsite labour abuses (evidence from the Sustainable Rescue Foundation, the Netherlands).

The availability of online information and self-identification mechanisms should be coupled with **awareness-raising campaigns**. La Strada International considers two types of campaigns as particularly important: (a) those directly targeted to potential victims and individuals at risk of exploitation and abuse; and (b) those targeted to stakeholders to recognise risks of technology-facilitated THB and report it. Different and Equal (Albania) and KOK (Germany) have highlighted the importance of educating ICT users about technology-related risks. They have suggested running wider campaigns to **raise awareness on how traffickers might exploit technology** and the risks at-risk individuals might face (particularly younger users). Emphasis should be placed on the recruitment, specifically on how a potential exploitative situation might begin (i.e., how traffickers establish initial contacts). Companies that provide online and ICT services should be made part to this effort. Migrant Rights Centre Ireland further noted that social media companies should work on deterrence.

Further, several NGOs, including La Strada International and Sustainable Rescue Foundation, have underlined the importance of increasing and improving **data exchange** among relevant stakeholders. These exchanges should include up-to-date knowledge about technology-related risks.

NGOs have stressed the importance of developing knowledge about ICT-related risks, and more generally technology-facilitated THB, also among organisations that assist victims, including counselling services. As **preservation of electronic evidence** is key to build strong investigations, it is crucial that counsellors and NGOs first-respondents are familiar with strategies to preserve digital evidence (e.g., by storing chat histories). Offering comprehensive training about data security and traceability on the Internet to counsellors and NGOs is seen as crucial.

FIZ (Switzerland) noted that ICTs, including social media and online information, can help NGOs establish contacts with potential victims and gather supplementary information about the circumstances of exploitation. If alerted to a suspicion situation, NGOs might **leverage the online information available to establish a contact with a presumed victim**.

Migrant Rights Centre Ireland and Astrée (Switzerland) have suggested establishing dedicated digital crime investigation units with expertise in technology-facilitated THB. Praksis (Greece) has called for stronger expertise among law enforcement authorities about ICTs and their risks. Furthermore, they have called for enhanced cooperation and exchanges among authorities and private companies.

Evidence from NGOs confirms that "**red flags**" for technology-facilitated THB cases are not widely used. NGOs report using standard indicators, but they call for a **review of such indicators** to take into account the specificities of technology-facilitated ICT – particularly in relation to recruitment and exploitation through ICTs. KOK (Germany) has suggested that monitoring of websites where clients exchange experiences of purchasing sexual services might provide hints of forced prostitution/THB. A review of "red flags" could include indicators applicable to such websites.

3.5.1. A focus on tech-based initiatives

La Strada International considers that its members and other NGOs are "increasingly" making use of technology. However, though "technical resources and opportunities have increased enormously", the extent to which NGOs utilise technology remains "limited". According to La Strada International, technology is mostly used to register data, and subsequently analyse it, and to monitor assistance activities. Increasingly, NGOs are using technology, including social media, to conduct campaigns (e.g., awareness campaigns; see below) and provide information, as well as to "get in contact with groups at risks or engage with communities online" (submission by La Strada International). As part of the current study, NGOs were asked to indicate examples of tech-based initiatives to enhance the detection of online and technology-facilitated THB, the identification of victims and the prevention of future cases. Below is a brief overview of such initiatives based on the evidence provided by NGOs.

Online self-reporting and contact with potential victims

- La Strada Moldova has indicated online mechanisms for children to self-report online safety issues (www.siguronline.md). These include unpleasant situations that a child might have been faced while on the Internet. The child will then be put in contact with a specialised counsellor and, if evidence of online sexual abuse or exploitation is identified, the case will be reported to law enforcement.

- In Switzerland, Astrée has observed an increasing number of victims self-referring to their services as well as of potential victims referred by friends or clients thanks to the organisation's online presence. Astrée also offers an online form to establish contact and request assistance. Further, FIZ has pointed to the successful use of social media platforms to establish contact with potential THB victims, if the name of the person is known. The website of the Swiss "National Platform against Trafficking" features links to a number of organisations that can offer assistance.

- Fair Work (the Netherlands) leverages social media to reach out to migrant communities to identify trafficked persons or exploitative situations. Fair Work first identifies Facebook pages that are relevant to a specific target group and then shares information through such pages. They create anonymous personal accounts, run by volunteers, that are used for prevention. As migrant workers often use social media to find information, the latter can be leveraged to help at-risk individuals "to become less isolated and more empowered" and reduce THB risks (submission by La Strada International). This is not always an easy task, though, as it is not always "easy for victims to know where to seek adequate information,

which information to trust; whom to contact and to find who can best help them, especially if they have little knowledge about the country and their rights in that country".

- La Strada International reported the development by some of its member of online chat consultation services to receive advice and report exploitation and abuse – besides the telephone-based helpline services.

- La Strada International also reported that its members normally utilise online platforms, such Facebook, Instagram, LinkedIn and their own websites, to inform about their work. Similarly, KOK (Germany) reported the use by its members of websites, Facebook and WhatsApp to disseminate information and establish a communication channel open to potential victims. Crucially, one organisation offers a WhatsApp number to clients to report signs of potential exploitation among sex workers.

Mobile Apps to raise awareness and seek help/information

- La Strada Czech Republic has been involved in the creation of SAFE, an app developed by IOM Slovakia in the form of an interactive game designed to prevent THB. By playing the game, users assess their risk vis-à-vis THB; the app also contains information about safe travel, foreign work and useful contacts in case of emergencies. Astra (Serbia) has developed BAN Human Trafficking, an app designed to make young people aware about the situations potentially leading to exploitation, and to provide advice on how to spot them. They are planning to upgrade it with a function to report exploitative practices.

- La Strada International has noted the development of apps by NGOs to report exploitation and abuse as, for example, the app developed by Unseen (UK). In Albania, Different and Equal participates in various mobile apps (e.g., "*#raporto #shpeto*") designed to assist victims of trafficking and gender-based violence ("*#GjejZa*").

- La Strada International further noted the development of apps to support vulnerable groups by, for example, providing access to information or employment rights in the country of destination. An example is Workenn App: A Game for Labour Market Integration of Migrants, produced as part of the Sirius Project to help migrant job seekers. As a non-European example, Apprise Audit is a platform developed by Mekong club and the UN University Institute in Macau, allowing for secure and confidential interviews of workers in the interviewees' own language.

Online awareness campaigns

- La Strada Moldova conducted an awareness-raising campaign during "Safer Internet Day 2019" aimed at raising awareness of sextortion among young people. People were encouraged to report cases via an online safe reporting mechanism (www.siguronline.md). The campaign reached around 70,000 online users. The same organisation tested profiling strategies to target their online messages by selecting the age category of online users, interests and profile.

- Different and Equal (Albania) conducted several online awareness campaigns using social networks and apps (including Facebook, Instagram, Twitter, Website and YouTube)

focused on the prevention of THB, sexual abuse and domestic violence (reaching around 15,000 users). A campaign was launched, together with other NGOs, during the Covid-19 pandemic.

- Novi put (Bosnia and Herzegovina) has run several awareness campaigns focused on the use of technology in relation to THB and child sexual exploitation.
- Astra (Serbia) has run campaigns raising awareness on the main ways of recruiting, including job offers on the Internet and grooming via Facebook and social networks, as well as strategies to control and exploit victims (including tracking victims through the use of location options available in widely used apps).

Further initiatives

- In 2018, Astra (Serbia) set up a "virtual girl" experiment—a profile of a 15-year-old girl navigating the Internet. Within 24 hours, this profile received over 3,000 requests, including job offers and explicit sexual offers from adult men (evidence submitted by La Strada International).
- Different and Equal (Albania) provides, as part of their reintegration programme, training on the use of computer and technology, which includes techniques of data protection.
- La Strada International noted some public-private initiatives in which NGOs are involved, e.g. a project launched by the University of Amsterdam with major Dutch banks to identify cases of trafficking. Dutch-based NGOs, including FairWork, CoMensha and La Strada International, were consulted as part of this initiative.

Looking forward and addressing critical issues

There is a large consensus among NGOs that more can be done to leverage technology, particularly to disseminate information, to approach and communicate with potential victims – as well as to receive tips and reports. FIZ (Switzerland) suggested to further develop tools to anonymously report violence and exploitation, and provide contacts with NGOs offering victim protection and counselling services. KOK (Germany) noted the importance of further developing visuals, e.g. videos, pictures and apps, to be used during training, as well as to be circulated online including among at-risk communities.

NGOs have also raised some **critical issues** related to initiatives and tech tools. La Strada International has pointed out that tech tools are generally produced as part of stand-alone projects and "often do not include testing periods". Thus, we are left with limited evidence about their effectiveness. Furthermore, when financial support for a project comes to an end, there is often no long-term financial strategy to promote and utilise the tools produced. This is particularly problematic as tools need "continuous updating and training".

La Strada International further noted that initiatives "often lack sufficient involvement of NGOs and other stakeholders that should use the tools in practice and therefore need to feel some ownership". It also pointed out that it still remains "unclear what the impact of technology has been on effectively preventing or combating THB", questioning whether "surveillance and profiling at borders as well as other locations [have] led to the actual identification of victims

of trafficking" and whether the persons identified through technology have then received "assistance and protection". They called for **more evaluation and impact assessment** of "all the technology tools developed". "Have these – often costly - tools served the needs of anti-trafficking stakeholders and have tools in fact been tested and well-used and if not, why not?", they asked.

Crucially, NGOs stressed that, overall, there is still limited availability of technological tools that practitioners can use. To suit the needs of NGOs, **tools need to be "cheap and easy to use"**. The Sustainable Resource Foundation further warned that "tools create a surplus of data for different users", hence it is important to develop them having in mind specific needs and a comprehensive strategy to avoid duplication of tools performing (easy) functions while lacking tools performing more strategic, complex, functions.

3.6. Evidence from tech companies

Facebook reported various **collaborations with NGOs** worldwide to create educational campaigns raising awareness about the risks of online sexual exploitation – particularly among young users – as well as the rights of potential victims of labour trafficking and domestic servitude. Such campaigns also provide information on trafficking hotlines offering help and support. As an example, Facebook indicated the Labour Trafficking/Domestic Servitude Awareness Campaign launched in March 2021 in partnership with Stop the Traffik, to provide information to domestic workers and low-skilled laborers in the Philippines about their rights, local recruitment guidelines for overseas job applications, and available helplines to avoid illegal recruitment and abuse.

Facebook also reported the creation of a shortcut to provide information and additional resources to people who search for terms related to sex trafficking. Such terms have been developed by internal and external experts.

To mitigate the issue of underreporting, Facebook indicated that they are working to "proactively find and take action on content related to human trafficking". They noted an "increase" in their ability "to detect violating content [which] results directly from major investments by our technical and operational teams".

IBM and Stop the Traffik, a UK-based NGO, have partnered in 2014 to create the Traffik Analysis Hub – a new entity running a **collaborative data sharing platform** underpinned by secure cloud and AI-based multi-lingual content analytics, and geospatial analytics. The Hub involves 95 organisations worldwide. The aim of the platform is to disrupt global human trafficking by bringing together NGOs (e.g., StopTheTraffik, LibertyShared, CrimeStoppers and Save The Children UK), law enforcement agencies (e.g., Europol, Interpol and various US police authorities) and financial institutions (e.g., Western Union, Barclays, Standard Chartered, Lloyds and Paypal). As noted by IBM, the Traffik Analysis Hub uses domain-specific custom AI (artificial intelligence) models to source relevant data at scale and classify this information based on a classification developed by the Hub expert community. Data are then shared among the participating organisations. One of the key outputs is the "Red-Flag Accelerator", a library of typologies developed from red-flag transactions identified in victims' accounts. Such red flag indicators are meant to be implemented in the monitoring systems of the participating financial institutions. Additionally, the Hub aims to develop a correlation-

based predictive tool to help identify the characteristics of communities at risk that may become sources of human trafficking.

IBM also noted a recently launched, **free online training roadmap** for people interested in becoming a data analyst in the THB domain. The training includes modules on human trafficking (Introduction to THB; how to spot signs of THB), as well as modules on data science and the application of technologies for data analytics.

IBM also sponsors online DataJam competitions during which IBM experts work with multi-sector teams to devise innovation in the application of technology for the disruption of human trafficking. Examples include:

- Tools to scrape online adult advertisement sites and apply markers of forced participation (e.g., third-party language, multiple advertisements using the same contact identifiers, advertisements relating to historically known victims' nationalities), and perform geo-spatial cluster analysis on the advertisements of "interest".
- Tools to scrape deep/Darknet marketplaces and forums messages, apply THB-specific markers via AI, identify trending topics and user handles, create network models of topics for further analysis by law enforcement agencies.
- Online job advertisement validator tools for smart phones, allowing individuals to verify the legitimacy of online job postings prior to engagement.

In relation to **cooperation with law enforcement agencies**, Facebook mentioned a number of Public/Private Partnerships (PPPs) they are involved in, such as the Interpol Human Trafficking Experts Group (HTEG), to tackle human exploitation. As a further example, Facebook reported implementing a Law Enforcement Online Requests System ("LEORS") to streamline legal requests for Facebook account data (including requests related to human trafficking). Requests submitted through LEORS are dealt with by teams based in the United States, Ireland and Singapore.

3.7. Further evidence from the landscape analysis

In addition to the evidence provided by State Parties, NGOs and tech companies, the study has also conducted a desk research of the current evidence base on the strategies and tools employed to combat online and technology-facilitated THB.

OCSE and Tech against Trafficking (2020) have conducted a survey of ICT tools and initiatives developed to fight human trafficking. They identified 305 tools/initiatives, developed by private sector companies, charities and governments (the vast majority in English). Of those tools: 26% are designed for victim and trafficker identification; 16% for awareness raising; 14% for supply chain management; 13% for data trends and mapping; 10% for corporate risk identification; 9% for worker engagement and empowerment and 12% for other purposes. The tools and initiatives surveyed by OCSE and Tech against Trafficking seek to accomplish the following set of goals: (a) dissemination of information to at-risk communities, including migrants; (b) education on THB risks, seeking help and reporting potential cases; (c) removing opportunities for exploitation; (d) identification of victims; (e) collection of

publicly available information to combat THB; (f) assessing risks of trafficking; (g) monitoring and compliance; (h) identifying and acting on typologies. Similarly, Raets and Janssens (2018) have identified the following (broad) ways in which tech-based tools can be used in fighting trafficking in human beings: (a) data aggregation and analysis; (b) blockchain for traceability and provenance (monitoring supply chains); (c) artificial intelligence (AI) and machine learning to yield high computational power; (d) facial recognition (web crawling); (e) tech for victims and survivors: identify and support victims, outreach in different languages. Muraszkiewicz (2018) has identified web crawling; data analytics; predictive policing; use of blockchain; geographic information systems (GIS); online databases; and crowd-sourcing initiatives as additional ways tech-based tools can be operationalised to combat THB. It is often unclear which of these tools really work, which ones can be usefully scaled up and which ones really produce benefits to victims of human trafficking (some of the tools surveyed appeared to have been designed to collect information that is then difficult to action). Information leveraged through technology needs to be acted upon. In the case discussed by Rende Taylor and Shih (2019), workers' reports via electronic (app-based) feedback on exploitation in supply chains were found to be hardly acted upon.

It has been stated in the literature that technology can hardly be seen a substitute for on-the-ground knowledge. Furthermore, according to law enforcement agencies interviewed by Elliott and McCartan (2013), mobile phone technologies including apps can be part of a toolkit to fight trafficking, but they are not a silver bullet. Operationally, Internet service providers are seen as the entities that hold an important share of electronic evidence, hence several sources have pointed to the importance of close cooperation with the private sector. Such cooperation should encompass mechanisms facilitating the acquisition of evidence, the removal of such evidence whenever appropriate and a prompt reporting to law enforcement in specific cases. At the same time, a number of obstacles to information sharing between different actors have been identified. These include data privacy and security issues. Calls for common international (multilateral) standards underpinning collaboration between law enforcement agencies, NGOs and the private sector have also been made.

Only a very small set of specific tools has gained multiple mentions in several sources. These include: (a) Project Artemis by Microsoft, which developed a tool to detect grooming techniques by creating a risk score for conversations based on past cases and then flagging up the most suspicious ones for human moderators to scrutinise; (b) PhotoDNA by Microsoft, which creates a unique digital signature (hash) of an image, which is then used to detect child sexual exploitation.

The International Trade Union Confederation reports of an awareness campaign run by AidRom to give information to people searching the Internet for jobs abroad. This campaign included tips on how to spot suspicious advertisements and developed the following guidelines: "1. Pay attention to the source of supply. Most specialized sites for job searches do not check posts from recruitment companies. 2. Never accept the offer that came from individuals. 3. Carefully read the mediation agreement. If you pay a fee, make sure that you know what you pay for and what you agree as conditions. Once signed, it is difficult—or impossible—to denounce. 4. Ask as many details as possible about the job for which you are recruited. 5. If a job seems too good to be true ... probably is not true!". The Internet is

leveraged as a tool to protect against abusive recruitment. It is not clear how long this campaign lasted and whether it has been scaled up or adopted in other countries.

Two projects are also often cited as example of good practices: Thorn's Spotlight and Polaris Project, both based in the US. Spotlight is a web-based tool developed to help investigators identify child victims of human trafficking by leveraging online evidence. There is, however, very scant information about the software in the public domain. The Polaris project analyses data mainly collected via a National Human Trafficking Hotline, supplemented with other (unspecified) sources of information.

Crowdsourcing the detection of victims is cited as a tech-enabled citizen's initiative, of which TraffickCam is often seen as a prime example. It asks people to take pictures of hotel rooms so that they can then be used to identify victims' locations. However, it is not clear whether such initiatives are effective. Furthermore, they might raise issues of privacy as well as the potential risk of vigilantism. While tips from customers are considered very valuable, crowdsourcing initiatives need to be closely scrutinised and balanced against the risk of creating virtual (and non-virtual) vigilante groups.

More generally, ICAT (2019) has identified a number of ways in which technology can have a positive role in tackling human trafficking. These include: (a) aiding investigations; (b) enhancing prosecutions; (c) raising awareness; (d) providing services to victims; and (e) shedding new light on the make-up and operations of trafficking networks. Various sources have pointed to the importance of '**digital footprints**', meaning that online contents and connected devices are an exceptionally rich source of information (Myria 2017; Mitchell and Boyd 2014). Crucially, it is possible to map **criminal networks** based on social networking sites (Myria 2017; also ICAT 2019 and TRACE 2015). The collection and analysis of digital evidence can **decrease the burden on victims** to provide evidence against traffickers (as well as evidence in their defence).

4. Training: what is provided, what is needed

4.1. Training for law enforcement: what is provided and what is needed

The study first explored the training currently provided to law enforcement in detecting and investigating cases of online and technology-facilitated THB. Next, it carried out a 'needs analysis' to identify additional training provisions that could be offered to increase the effectiveness of detection and investigation, and the identification of victims.

Broadly speaking, different countries provide different levels of training to law enforcement, delivered in different formats. Overall, the vast majority of countries report delivering training on THB. The audience of such training, however, varies among countries, with some requiring all police officers who might come into contact with a potential victim to undergo such training while others limit the training to specialised units.

What are the training elements that countries consider crucial in relation to online and ICT-facilitated THB? There is a consensus on the fact that officers need to receive training on (a) on how to detect cases and victims; (b) how to collect, store and process **electronic evidence**, including methods of extracting information from computers and other digital

media; and (c) how to use relevant pieces of software, including **Big Data Analysis** and web-crawlers (where allowed by domestic legislation). **Training on OSINT** is seen as essential by several countries. Investigative techniques involving **covert online investigations** are also seen as crucial.

While the vast majority of countries has reported providing elements of this training, they have also flagged up some issues, including: (a) the need to keep the training up to date and, in some cases, to considerably enhance the current provisions; and (b) the need to increase the proportion of personnel that receive training. Some countries have expressed concerns about the limited training that is often provided in relation to ICT-related issues and, even more, ICT-facilitated THB. It has been suggested to **devise and provide intensive training courses on ICT-facilitated THB**, covering also technical issues. Again, different countries would find themselves in a different position in relation to the digital competencies of their law enforcement personnel, but a number of countries have suggested the need to offer **further training on the use of ICTs** to enhance the detection of THB cases.

Countries have also pointed out the need to deliver both initial and continuum training taking into account the fast-changing investigative landscape. This, in turn, requires resources for the preparation of training modules (including research on new developments in the context of ICT-facilitated THB) and their delivery.

It is not uncommon for State Parties to have their officers attending training modules organised by international organisations or by other countries. Exchange of information and knowledge at the international level is certainly a good practice. In addition, for countries with limited budgets and resources, the benefits can be considerable. However, as some training elements remain very much context-specific, there is a need for all countries to be in a position to develop knowledge internally and to offer training that *also* considers the local specificities of the phenomenon (a limited number of countries does not currently organise any training on THB and ICT-facilitated THB, including on OSINT, but only relies on training provided by external organisations).

Different countries present different organisational set-ups, particularly when deciding where ICT knowledge sits. However, it is crucial to note the importance of avoiding bottlenecks in the daily operations due to the non-optimal distribution of skills. For example, it is important that **knowledge is not structured in silos**, thus hampering effective investigations. A solution envisaged is to think of a two-way training system between officers specialised in THB and officers specialised in ICT. Another strategy is to disseminate a certain degree of ICT skills among different units, including THB units. Looking ahead, **the risk of bottlenecks** is particularly acute. As ICT-facilitated crimes, including THB, are likely to increase, there is a need not to over-rely on centralised cybercrime centres. Ideally, such centres should only be called upon in cases characterised by a very high level of technological sophistication – *which does not seem to be what a typical case of ICT-facilitated THB looks like*. In order to avoid bottlenecks in the system, it is crucial to include general/basic **'cyber' knowledge in routine training** provided to investigators rather than seeing this as a set of 'specialised' skills.

Based on the evidence from State Parties, we can identify six broad areas that are seen as critical for capacity building. These include:

- Collection and analysis of open-source information (OSINT).

- Data collection from social network profiles and communication applications, as well as from Darknet/TOR network.
- Examination of information present on communication and information storage devices, including information deleted by users, as well as knowledge on encryption.
- Ability to corroborate data acquired from ICT sources with additional evidence acquired during the criminal investigation.
- Identification of victims/potential victims in the online environment.
- Economic and financial crime training with an element dedicated to online transactions and potentially cryptocurrencies.

4.1.1. Designing future training and good practices

The evidence from State Parties points to a number of concrete initiatives that could be adopted to strengthen training provisions in the context of online and technology-facilitated THB. Below are some suggestions on the design of future training modules.

- Creation of THB-based case studies and scenarios to be included into a **'digital investigative' training**. Such training could be divided into two levels: Level 1 could be delivered to all frontline officers, while Level 2 could include advanced provisions delivered to a smaller set of learners. It is conceivable that at least a portion of this training would take the form of small group learning to foster the exchange of ideas and discussion of practices.
- **Adding an ICT element to existing THB training**. While several countries have mentioned providing THB training, only a minority has expressly indicated the inclusion of ICT-focused elements in this training. As more and more interactions take place online, it is crucial to include ICT elements to the 'traditional' THB training. Technical training can include elements on best practices in investigating ICT-facilitated THB, as well as national and international experiences.
- Delivery of joint training activities involving multiple countries designed with consideration for actual trends. For instance, if there is evidence that victims tend to be recruited in country A and then exploited in country B, it could be beneficial to organise a joint training activity involving officers from A and B. Echoing Joint Investigation Teams (JITs), we could label such activities **JTAs ("Joint Training Activities")**.
- Recruiting non-sworn officers possessing technical skills. Those officers can integrate specialised units (e.g. THB units), develop knowledge on technical ICT issues internally and disseminate it within the unit/organisation.
- Organising joint training sessions **bringing together specialised investigators and prosecutors** to familiarise both sets of actors on the possibilities offered by new investigative methods, e.g. the use of cyber-infiltration or online covert operations, as well as the collection of electronic evidence (including virtual assets seizures). Such training can cover both technical and legal aspects with a view of enhancing the use of new ICT-oriented methods among investigators and prosecutors.
- **Knowledge sharing at the international level**, e.g. through participation in international/regional training focused on specific aspects of investigating ICT-facilitated THB (examples cited by State Parties include the seminar "International Cooperation in Cybercrime

and Electronic Evidence" organised by the Council of Europe and the EU Cyber@East Joint Project delivered on 7-9 December 2020).

Countries have identified a number of concrete initiatives as examples of good practices:

- In Austria, the Joint Operational Office against Trafficking in Human Beings and Human Smuggling (a sub-department of the Criminal Intelligence Service) organises training and seminars on trafficking in human beings, cross-border trade in prostitution and identification of victims. Specific training was provided to the Austrian Police, the judicial authorities, the Federal Office for Immigration and Asylum (BFA), the Federal Administrative Court (BVwG), financial authorities, labour inspectorates and legal counselling services on detection of online cases of THB, including on social media. Crucially, such training went beyond law enforcement and included the labour inspectorate, counselling services and financial authorities. Furthermore, police officers specialised in ICT received specific training focused on THB for sexual exploitation. On the other hand, officers specialised in ICT provided training to colleagues specialised in THB/cross-border trade in prostitution with the Criminal Intelligence Service/CIDs. This is a good example of the two-way training discussed above – and a template that could be potentially replicated elsewhere.

- In Bulgaria, in 2020, a series of specialised workshops for police officers, prosecutors and judges discussed the investigation and prosecution of THB cases using open-data sources, including online data.

- As part of partnership agreements with Romania and Bulgaria in the field of THB, Norway will organise two joint Open Source Intelligence (OSINT) training activities for Romanian and Norwegian participants. The aim of the training is to enhance the ability of investigators in Norway, Bulgaria and Romania to identify and investigate ICT-facilitated THB.

- In Greece, cybercrime training and education initiatives take a two-pronged approach: (a) a set of university courses to improve understanding of cybercrime among the next generations of scientists and law students, and (b) a set of shorter training courses for law enforcement personnel, judicial authorities and private sector employees to improve their understanding of cybercrime and their day-to-day responses.

- In Britain, law enforcement authorities have formal standard operating procedures (SOPs) or other guidance on pro-active monitoring, detection, investigation and disruption of ICT-facilitated THB. These include: mapping online platforms where the risk of THB is high; conducting undercover operations online; using specific indicators of potential THB on online platforms; analysis and management of reports received through hotlines for online child sexual abuse and exploitation; the use of specific technological tools to fight THB. Additionally, investigators receive training on how to effectively layer open-source information with a variety of forms of intelligence.

- In France, the first level training to police officers includes modules on: basics on digital investigation; anonymity, darknets and virtual currencies; landscape analysis of cybercrime offences; investigating the Internet and social networks (this is normally followed by a specialisation on a topic, e.g. fraud or child sexual abuse); first responders in cybercrime (i.e., preservation of a digital crime scene). Further specialised training includes modules on:

cybercrime investigations (collection, processing and analysis of evidence from mobile phones and computers; judicial investigation acts related to digital technologies, including legal issues, international cooperation and investigative strategies); Digital Trace Analyst training; phone data acquisition; investigation under pseudonyms. A one-week training dedicated to THB for the purpose of labour exploitation is currently being created (with a view of launching it in the first half of 2022). This training will include a module dedicated to the use of technological tools.

4.2. Training for prosecutors and judges

According to the evidence submitted, the provision of training to prosecutors and judges in relation to ICT-facilitated THB is rather uneven across State Parties. Several countries have indicated that they are not currently providing any training on the phenomenon to the judiciary. Other countries provide general training on THB without any element specifically focused on ICT-related issues. Another set of countries has indicated that they provide training on how to use international legal instruments in the context of cybercrime, e.g. the Budapest Convention and the connected domestic legislation and/or on how to build cybercrime cases. Finally, a group of countries has included elements of cryptocurrencies and knowledge of specific technological tools in their training. Ideally, all countries should **move towards integrating training on ICT-related THB, the use of international legal instruments in the context of cybercrime**, as well as the implications of the use of specific technological tools in investigating THB cases (e.g., web-crawlers or software to decrypt information).

A minority of countries appear to have integrated in their cybercrime training case studies related to THB. Similarly, a minority of countries have indicated that they are providing training that includes both THB and ICT elements.

Countries have identified in their replies to the questionnaire a number of concrete initiatives as examples of good practices:

- In the Republic of Moldova, during the first semester of 2021, the National Institute of Justice has delivered training to 110 attendees covering aspects of investigations into ICT-facilitated THB. The training included sessions on (a) "peculiarities of investigations and trials of crimes related to trafficking in human beings and bodily elements"; (b) "peculiarities of investigating and prosecuting crimes in the field of combating trafficking in human beings; (c) "peculiarities of investigations and trials of cases concerning cross-border, transnational and organized crime".

- In Bulgaria, the Prosecutor's Office of the Supreme Court delivered seminars to investigators and prosecutors on THB and the use of ICTs in THB. The Prosecutor's Office maintained that "workshops delivered by experts in the field of ICT are especially effective, presenting practical examples of using software programmes as well as the possibilities and operational tools of using mobile apps to uncover serious crimes".

- In Sweden, there are prosecutors specialised in ICT, some of whom deal with THB cases. The Prosecutorial Authority organises internal training on conducting investigations on ICT-related criminality (including the use of crypto-currency in criminal activities). Numerous prosecutors who deal with THB cases have participated in these training sessions. Further,

the Judicial Training Academy, which is part of the Swedish National Courts Administration and is responsible for judicial training of judges and other legal personnel, offers training on ICT-facilitated crime pitched at different levels.

- The Latvian authorities have referred to the international training on human trafficking and cybercrime organised by the Polish Prosecutor's Office and delivered to prosecutors specialised in organised crime (21-23 October 2019 in Krakow).

Finally, a few countries have highlighted the importance of enhancing the training of judges and prosecutors in relation to electronic evidence.

BOX | Training for NGOs

NGOs provide key training and expertise based on their day-to-day experience assisting and counselling victims – including to law enforcement and at-risk communities and individuals. However, they have expressed the need to also receive training from law enforcement authorities and international organisations on the latest developments in both the technological and the THB landscapes, including changes in recruitment strategies.

They also flagged up the need for training on best practices and sharing of experiences among countries. This is particularly relevant to the design and coordination of campaigns involving both origin and destination countries.

While some NGOs have specialists on online safety issues, overall there remains a lack of training on technology, including the use of specific tools to identify and assist victims. As pointed out by La Strada International, this is "due to lack of resources and capacity" as it is "already difficult to get sufficient funding for core support programmes".

5. Legal instruments

This chapter explores the international legal instruments relevant to combating online and ICT-facilitated THB. An overview of the country-specific legal frameworks related to the identification and removal of THB-related content as well as of domestic legal instruments relevant to combating THB more generally is available in the Web Appendix.

5.1. International legal instruments

State Parties have identified a number of legal instruments as relevant to combatting ICT-facilitated THB. Most of the instruments are general and aimed at tackling THB regardless of the *modus operandi* of the traffickers. The most relevant instrument geared towards ICT-facilitated crime is the CoE's Budapest (Cybercrime) Convention, which is cited by several State Parties as an "important" tool. Given its relevance, the use of the Cybercrime Convention

in the context of THB is discussed in a separate section below. Additional instruments identified by State Parties are the following:

- UN Convention against Transnational Organized Crime and its Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children (2000)
- CoE European Convention on Extradition (ETS No. 024)
- CoE European Convention on Mutual Assistance in Criminal Matters (ETS No. 030)
- CoE Convention on Action against Trafficking in Human Beings (CETS No. 197)
- Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims
- Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

On the related issues of child sexual abuse:

- CoE Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention, CETS No. 201)
- Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography
- European Union Council Decision of 29 May 2000 to combat child pornography on the Internet 2000/375/JHA.

On labour exploitation:

- International Labour Organisation, Convention No. 189 and Recommendation No. 201 Concerning decent work for domestic workers, 2011
- International Labour Organisation, Protocol of 2014 to the Forced Labour Convention, 1930.

In addition, State Parties have identified a number of international agencies and programmes instrumental in enhancing international legal cooperation, also in the context of ICT-facilitated THB. These include:

- Interpol
  - IWOL Project (blocking of domains related to child sexual exploitation)
- Europol
  - EMPACT (THB)
  - Joint Action Days
- Eurojust
- Selec (Southeast European Law Enforcement Centre).

Finally, a set of specific operational instruments emerges from the evidence submitted by State Parties. This set includes the following instruments:

- Legal assistance requests
- European Arrest Warrant
- European Investigation Order
- Joint Investigation Teams
- EU Prüm system (exchange of national DNA, fingerprint and vehicle registration data)
- EU Passenger Name Record (PNR)
- Europol SIENA
- Liaison officers
- Interpol Notices System.

5.1.1. Gaps in the current framework

Overall, State Parties have expressed a positive and supporting view of the available legal instruments enabling cooperation among countries in combating THB. The CoE Conventions on (a) Mutual Legal Assistance and (b) Cybercrime are considered among the "most commonly" used instruments and, overall, they are judged as "adequate". Nonetheless, State Parties have identified some potential gaps and areas in which the current legislation might be improved. Please note these gaps reflect – and complement – the challenges related to the investigation and prosecution of ICT-facilitated THB already discussed in Chapter 1 – and should be read in conjunction with such analysis.

The main gaps identified by State Parties relate to:

- Absence of a commonly agreed (standardised) legal environment underpinning exchange between Internet service providers and authorities when dealing with specific investigations.
- Provisions that allow for a more timely response from private companies to data requests to avoid long delays in the delivery of such data. However, such provisions need to take into account that very tight timeframes might penalise small providers to the benefit of large providers as the latter can more easily afford expensive automated systems and/or on-call services (as highlighted by the Swiss authorities).
- Provisions to compel private companies to disclose information upon direct request/order from another country.
- Provisions implementing shared rules on data retention.
- Provisions to facilitate the collection of victims' testimonies and their use in a different country. This would alleviate the difficulties countries face in convincing victims to testify in trials due to a host of reasons, including the mobility of victims, difficulties in locating them and continuing vulnerability.
- Provisions around encryption (e.g., providers are not obliged to remove encryption when handing over materials to authorities).
- Issues around transnational measures targeting websites hosting materials that can be linked to the facilitation of victims' exploitation. This is a particularly complex issue as it is

closely intertwined with differences among State Parties in their approach to prostitution activities – and the different regimes adopted in different countries.

- Provisions introducing a duty of vigilance by companies on their entire supply chain, targeting for instance the use of ICTs in the context of recruitment (by way of examples, France's Law n° 399/2017 on the duty of vigilance and the 2015 UK Modern Slavery Act introducing a duty of transparency in supply chains).
- Use of terminology that not always allows for legislation to evolve in parallel with changes in traffickers' *modus operandi*.
- Differences in the transposition of the THB offence (as per the UN Palermo Protocol) in domestic legislations. These differences might pose challenges to international cooperation, for example around issues related to lack of consent and victim's coercion.
- The European Arrest Warrant is seen as a valuable tool; however, some relevant countries of origin are often outside the EU Judicial Framework.
- European Investigation Orders (EIOs) can lack flexibility, e.g. there might be a need for a new EIO if the investigation takes new directions, and they can be subject to long response times.
- Joint Investigation Teams (JITs) are seen as "effective" means; however, they can be (a) complex to implement; and (b) they require a mirror investigation in the partner country(-ies).

5.2. The Budapest (Cybercrime) Convention and the fight against ICT-facilitated THB

There is a large consensus among State Parties on the value of the Cybercrime Convention – with many countries indicating it as a "very valuable tool". Several State Parties consider the Cybercrime Convention as a key **supporting tool** in the fight against ICT-facilitated THB.

According to the evidence submitted, State Parties consider the provisions related to **procedural law** as the most valuable in the context of ICT-facilitated THB (Chapter II, Section 2 of the Convention) rather than the substantive criminal law measures provided in Chapter II, Section 1. Crucially, the scope of procedural law provisions was not made dependent on the commission of a criminal offence listed under the Section 1 of Chapter II. Cases of ICT-facilitated THB are likely to fall either under "criminal offences committed by means of a computer system" or, at least, offences that require the "collection of evidence in electronic form" (Article 14, para 2). Similarly, Article 23 states that the principles underpinning international cooperation in the context of the Convention apply to "investigations or proceedings concerning criminal offences related to computer systems and data, *or* for the collection of evidence in electronic form of a criminal offence" (italics added). State Parties have highlighted the **importance of non-restricting procedural measures to offences explicitly listed** (e.g., those in Chapter II, Section 1). However, not all the countries seem to agree on this wider interpretation of the scope of the Convention.

The Convention clearly achieves its full potential only when it is not restricted to the offences explicitly listed in Chapter II, Section 1. This is particularly true in the context of ICT-facilitated THB. As noted by the Finnish authorities, among others, "the substantive criminal law provisions of the Budapest Convention [that] cover computer-related offences, such as illegal access, data interference, computer-related forgery and copyright infringement and other

comparable offences, are only rarely or not at all relevant in the context of THB". On the contrary, several State Parties have indicated that they have relied on the Convention's provisions on data preservation in the context of THB investigations (particularly the Articles 16-21).

Several countries have indicated the utility of provisions included in Chapter III of the Convention (on international cooperation) as a legal basis for gathering and sharing electronic evidence across countries. The mutual assistance mechanisms provided for by Chapter III of the Conventions (Articles 29-34) are deemed "useful". A few countries have expressly indicated that they had previously relied on them. Article 29 and 31 have received the most references; Article 30 has not been explicitly mentioned in the submissions; nonetheless, it might offer a useful tool in the context of ICT-facilitated THB.

The establishment of a 24/7 **network of contact points** (Article 35) is also seen as an important provision, particularly in the context of collecting electronic evidence. It is crucial, however, that contact points are easily accessible from within each country. This speaks to the **issue of bottlenecks within a system**. Where the contact point is located within the criminal justice system is key – and it can be very consequential. Different models apply. In the Republic of Moldova, for instance, such contact point is located within Directorate of Cybercrime Investigations; in Malta with the Police Cyber Crime Unit and, in Poland, with the Bureau for Combating Cybercrime of the National Police Headquarters. In France, it sits with the Central Office for Combating Information and Communication Technology Crime (OCLCTIC) while in Latvia such contact point is located with the International Cooperation Department of the State Police. The authorities in Bosnia and Herzegovina have explicitly mentioned their "very positive experience" deriving from the 24/7 contact point "not being located within the unit dealing with cybercrime". Looking forward, it is likely that, with the increasingly central role played by ICTs and the electronic evidence, such contract points will be under increasing pressure – and quickly overwhelmed if not adequately staffed. Stand-alone support units would perhaps be preferable to cyber-crime units – ideally staffed with personnel possessing expertise in different areas and crime types, including ICT-facilitated THB. However, no matter the model chosen, country should be mindful of the issue of bottlenecks.

5.2.1. Looking ahead: how the Cybercrime Convention can be further used to fight THB

Several countries have highlighted the importance of the Second Additional Protocol to the Convention. It has been indicated in several submissions that the Second Additional Protocol will create valuable tools for law enforcement – to be used also in the context of ICT-facilitated THB – enhancing cross-border criminal investigations and further improving cooperation in relation to securing electronic evidence. Articles that have been highlighted as particularly relevant entail include provisions related to joint investigations, including Joint Investigation Teams; expedited disclosure of stored computer data; emergency mutual assistance and direct disclosure of subscriber information.

Further, State Parties have suggested the following actions to improve the fight against ICT-facilitated THB through the use of the Cybercrime Conventions:

- Full harmonisation of all national legislations with the Cybercrime Convention to leverage on the full potential offered by the latter.
- Wider and enhanced training on the possibilities offered by the Cybercrime Convention. It transpires from the submissions that not all State Parties are currently using the tools included in the Convention to their full potential.
- More clarity on the scope of the procedural provisions already included in the Convention and its Additional Protocols as some degree of disagreement among the State Parties on the extent to which current provisions can be applied to THB cases has emerged. While some State Parties are of the view that, as long as electronic evidence is involved, the Cybercrime Convention can be fully leveraged, others have cautioned that the use of the Convention and the Protocols, including the Second Additional Protocol, requires "suitable cases" (what makes a case "suitable" has not been specified in the submissions).
- Some State Parties have expressed the view that the Second Additional Protocol needs to include provisions strengthening the sharing of electronic evidence, improving the modalities of mutual legal assistance, fostering cooperation with Internet service providers and improving cross-border access to data.
- A minority of State Parties are of the view that the Cybercrime Convention should be supplemented or amended to explicitly include THB in its scope. The Bulgarian authorities have expressed the need to draw up "a catalogue of crimes" to which the tools included in the Cybercrime Convention and the Additional Protocols can be applied. However, this view does not seem to be widely shared among State Parties as there appears to be a general preference for a broader interpretation of the scope of Convention based on the (broad) requirement of "collection of evidence in electronic form" (see also above).
- The Slovak authorities have suggested the implementation of a procedure to accelerate provision of MLA by allowing for the possibility to send a request directly to an entity located in the jurisdiction of a foreign country provided that the judicial authority of that country is notified.

BOX | Challenges Identified by NGOs

Generally speaking, NGOs are of the view that challenges are mostly a consequence of the implementation of the current provisions, including due to the lack of resources available to law enforcement and support organisations, rather than by the letter of current legal provisions.

La Strada International noted **"clear restrictions" introduced by data protection legislation (GDPR) and privacy rules**. An example is the "EU proposed e-privacy legislation which stopped tech companies from scanning for child sexual exploitation online" (now temporarily suspended following oppositions by many CSOs). Sustainable Rescue Foundation pointed to a "clear transition from physical evidence to digital data" which creates the need for "digital forensics as admissible evidence for police and prosecutors" in all jurisdictions. Further challenges they have identified relate to the EU GDPR; updating regulations and case law to take into account cybercrime and the Internet; devising legislation and operating rules tailored to digital investigations.

Sustainable Rescue Foundation also suggested looking at legislation against financial crime as a solution to the problem of converting information into admissible evidence. For example, the South African Anti-Money Laundering Integrated Taskforce, which is a partnership between public entities and the financial sector, can apply for a judicial warrant authorising access to relevant information held by financial and other institutions. Through an affidavit this information (i.e., the financial analysis of the judicially obtained financial information) can then be used by law enforcement agencies.

6. Human rights, ethics and data protection

6.1. Evidence from State Parties

With regards to **data processing and data protection**, all State Parties have noted the adoption of Data Protection Laws – often harmonised with the EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (also referred to as the European General Data Protection Regulation: GDPR) and/or the CoE Convention for the Protection of Individuals with Regard to the Processing of Personal Data (ETS No. 108, revisited in 2018 as version 108+). The principles behind data protection are similar across State Parties. These include legality, purpose limitation, data minimisation and proportionality, accuracy, storage limitation, integrity and confidentiality. It is not possible to conduct an evaluation of the implementation of such principles based on the evidence provided in the replies to the questionnaire.

Regarding **human rights** and **personal protection of victims**, a number of countries noted the introduction of measures to prevent offenders from making contact with victims; the questioning of witnesses through videoconferencing to prevent contact with defendants; and in some cases the possibility for victims to give evidence in court anonymously to protect their anonymity. Victims can be placed in **shelters** and given **assistance**.

In France, users of the platform for reporting sexual and gender-based violence need to **consent to the collection of personal data** when they first connect to the platform. This consent is renewed throughout the conversation. However, it is not compulsory to provide one's identity in order to access the chat room – hence allowing for anonymous contacts.

As for **data collected during police work**, including investigations, State Parties have highlighted that laws and regulations normally stipulate that such information is subject to confidentiality and can only be shared under very limited circumstances following strict procedures and authorisations. State Parties have indicated that the rules according to which police forces can register data in specific databases are normally harmonised with the EU Police Directive. Individual countries can have more stringent national requirements. As pointed out by the Norwegian authorities, special categories of personal data, e.g., on sexual orientation, religion and political views, may be subject to additional requirements, and "may only be processed when 'strictly necessary' for defined purposes.". Normally, the same set of rules and safeguards covers all investigations and intelligence work, including those involving ICT-facilitated THB. It is crucial that law enforcement personnel is adequately trained on the regulatory and ethical provisions governing the processing of personal data.

Police work also needs to **balance different needs and rights**. For instance, as noted by the Finnish authorities, an order limiting access to electronic communication "can only be issued if the benefits of prohibiting the access to information can be considered to be significantly greater than the restrictions on the freedom of expression and other fundamental rights of network users" (Section 185 of the Act on Electronic Communication Services 917/2014). Additionally, it must be "technically implemented in such a way that the protection of the confidentiality of communications is not compromised". More generally, Section 226c of the same Act stipulates that "measures related to terms of use of video-sharing platforms shall be proportionate to the nature of the content in question and take into account for

example the potential harm and the rights of service providers and users". The Finnish National Bureau of Investigation has self-identified privacy issues on the use of outsourced technical tools and has reported these to the National Police Board.

State Parties have indicated they have **age-sensitive protocols** in place, referring to different sets of procedures and safeguards applying depending on whether a victim is a child. For instance, children are normally hosted in separate support centres; different techniques and interrogation rooms are used, often with psychologists present. In some countries, criminal proceedings involving children are conducted exclusively by police officers specifically trained to work with children and juveniles.

6.2. Evidence from NGOs

NGOs have stressed the importance of – and awareness about – data protection rules, confidentiality, safe storage as well as procedures around consent.

Evidence from several NGOs indicates that, as a standard procedure, organisations ask for the victim's consent before sharing information with law enforcement. As highlighted by FIZ (Switzerland), this consent also extends to sharing SIM card details and social network credentials. La Strada International stated that all their members "do not pass on any information to the police without the victim's consent, unless there are dangerous situations where action is urgently needed". An issue arises when victims are reluctant to file a complaint with the police "out of the risks this will entail, including risks that their situation becomes known to others, next to risks of retaliation". La Strada International estimates that this is the case for "many trafficking victims".

Different and Equal (Albania) mentioned the use of security protocols in any communication with law enforcement agencies, including encryption. Internal protocols are built taking into consideration the need to maintain victims' confidentiality and protect their data. Similarly, FIZ (Switzerland) has stressed the need to protect data confidentiality as a requisite for good cooperation with law enforcement. Astra (Serbia) noted that **victim confidentiality** is "a crucial part of our work" and waiving it "is not and must not be a condition to receive support and assistance". KOK (Germany) pointed out that "the protection of an individual ranks higher than the need to collect evidence". Praksis (Greece) maintained that, when sharing information with law enforcement within the framework of data protection rules (consent-based sharing), their "primary concern is always the immediate and effective protection of a potential victim".

Issues of data protection and data sharing can generate **moral dilemmas**. As pointed out by La Strada International, sharing data with law enforcement and filing complaints does support investigations, which in turn can potentially save and protect more victims down the line. However, this can come with a cost to the individual victim, who might be exposed to risks and threats, including social exclusion. Further, there can be issues related to the long-term effect of registering a victim and sharing personal data, including potential prosecution and punishment by the authorities (this can be exacerbated when a victim happens to be in a country irregularly at the time of the registration). Both La Strada International and La Strada Moldova consider that finding the right balance between the victims' need for confidentiality in accessing services and the need to collect evidence to assist the fight against

THB more broadly can be "very challenging". This is even more acute when the victim is a child: as noted by La Strada Moldova, children are often afraid of granting consent and fill in a formal complaint with the police, including due to the fear of their parents' reaction.

According to La Strada International, data protection rules "have made data sharing among NGOs and other relevant stakeholders more difficult". At the same time, NGOs are aware that it might be difficult for "victims of THB or at-risk groups to know which data is kept, and/or to ensure that data is rectified, erased, blocked or deleted and to enforce this right", despite data protection protocols being in place.

Further issues emerge from the collection of identifiable personal information via **data extraction techniques**. The Sustainable Rescue Foundation (SRF) referred to two separate projects currently running in the Netherlands: RIVET (SRF) and *Lovitura 10 Elenas* (Dutch Police lab). Both projects focus on trafficking of Romanian women to the Netherlands for sexual exploitation. SRF RIVET uses victim-centred data extraction based on interviews with 10 Romanian sex workers, and explores the use of technology for data discovery, collection, cleaning, and analysis to build taxonomies of *modus operandi*. *Lovitura 10 Elenas* digitally follows ten Romanian sex workers to gain an understanding of criminal networks. As pointed out by RSF, the challenge is "how to ensure [that] all Romanian sex workers participating in both projects remain anonymous". Shelters are keen to protect the anonymity of sex workers and police cannot share their operational database. SFR has suggested the use of multi-party computation (MPC) data comparison as a possible solution. This approach consists in anonymising data coming from different datasets (e.g., NGOs and police) in such a way that they can be then shared and read by different systems to check, e.g., for name duplicates.

La Strada International called for more attention to the potential risks and harm generated by (large scale) data collection and tech tools, cautioning that, at the moment, the focus is only "on the positive aspects and opportunities" of such tools. The same organisation also maintained that "more control is needed on the use of data and secured storage and ensuring that all data protection rules are effectively followed". Victims, at-risk groups and NGOs should have "more possibilities […] to reject data requests and minimize data collection".

NGOs tend to have different protocols in place based on whether the victim is a child or an adult (**age-sensitive protocols**).

6.3. Further Evidence from the Landscape Analysis

ICT can have a considerable impact on the **human rights** of individuals, including the rights to privacy, freedom of expression and freedom from discrimination. A number of issues have been raised in the literature.

Based on OCSE (2020), we can list a number of **ethical issues** to be considered when developing technology to combat human trafficking. These include: (a) protection of data privacy; (b) consent protocols signed by victims; (c) training for people handling sensitive data, particularly victims' data; (d) secure storage of data; (e) preventing the use of technology for obtaining sensitive data about vulnerable people (blanket collection of data over vulnerable or marginalised populations, creating risks of discriminatory practices); and (f) using technology in a way that does not infringe human rights of victims as well as those

of the general population. ICAT (2019) also stress issues related to **data privacy, ethics, transparency, accountability and informed consent**. They emphasise the need to ensure that data are stored securely; that consent protocols are in place; and that those are gender- and age-sensitive. Further, information released by law enforcement needs to be assessed so that victims and their families are not put at risk.

ICAT (2019) and other sources have pointed to the sensitivity around **data sharing**. When data is shared between countries and/or relevant agencies, it needs to be done in accordance with the principles of privacy and confidentiality. It is noted that a potential conflict might arise between the need for confidentiality when victims access services and receive support on one hand, and the need for information/evidence to build strong investigation on the other. Gerry et al. (2016) have stressed the importance of key legal principles – the fair information principles – in relation to personal data processing (these includes the principle of purpose limitation). It is suggested that such principles also remain important in the case of human trafficking, and specifically in relation to victims.

Gerry et al. (2016) also warned about the risk of widespread **tracking tools** to combat human trafficking. While such technology can offer new opportunities to intervene in trafficking situations, it also consists of **a form of surveillance that is potentially highly invasive** on a person's privacy. As they write, it "can reveal plethora of information regarding their personal life, including their affiliation with a particular religion, the development of personal relationships and associations with other individuals as well as their everyday habits", thus placing vulnerable groups at risk of discrimination and profiling. Blanket monitoring of entire at-risk populations, e.g. migrant groups, can have serious repercussions on the privacy of individuals. Gerry et al. (2016) stress the need to develop **mechanisms to ascertain that tracking technology is not used excessively or abused**. They suggest avoiding systems that involve centralised storage of personal data of victims or potential victims. More generally, technology-based tools to fight human trafficking need to be **developed and used responsibly and ethically**. Such requirements need to be considered during all stages, from the development to the final use. Technology-based solutions also need to be judged against their level of invasiveness in people's privacy. Some scholars, including Milivojevic et al. (2020), have warned about the potential adverse consequences on marginalised population of large-scale use of facial recognition techniques, and more generally of what they define "the moral imperative to 'protect and rescue' ". While they acknowledge the potential for technology to assist in the fight against human trafficking, they also stress the importance of placing the **best interests of victims** at the centre of any action.

A few sources, including Milivojevic et al. (2020) and Gerry et al. (2016), have highlighted the importance of **not cutting victims out of technology**, as access to technology can be their only way to communicate with the external world, and may serve as an important coping mechanism. Removing access to technology can be disempowering to victims; promoting safe access to technology should be privileged instead.

Finally, there is **little recognition** in the literature about **gender-based sensitivities**. It is acknowledged that the type of exploitation is gender-sensitive, with women more often exploited for sexual services, domestic work and personal care, and men more often exploited in agriculture, construction and other manual occupations (e.g., corner shops, car washing). Further, it appears that online grooming is more associated with female victims than male

victims; however, the evidence also suggests that other vulnerabilities might be at play in the case of online grooming, for example a person being in a care institution (preliminary evidence from Romania is included in Di Nicola et al. 2017).

Recommendations

Actions to enhance detection of technology-facilitated THB cases

1. Law enforcement should invest in capacity building in the areas of **Internet monitoring**, **cyber-patrols**, **undercover online investigations (cyber-infiltration), the use of OSINT by specialised officers**, **social network analysis**, and the use of **automatic searching tools** to analyse evidence. The development and use of such tools must adhere to the rule of law principles. Countries should consider adapting existing legislation to allow for cyber-patrolling and covert online investigations (cyber-infiltration) – with careful consideration for ethical implications. Authorities should also consider investing in tools to assist investigators in handling and processing large-volume data (big data capabilities). Resources could be pooled at the supranational level for the development of technological products, such as web-crawlers as well as sharing expertise on their use.

2. Law enforcement and labour inspectorates should implement **more stringent regulations and frequent controls on job advertisement websites**. This could be done with the support of technological tools developed in cooperation with private companies (e.g., online job advertisement validator tools, tools to scrape job advertisements sites and apply THB markers). Labour inspectorates **should develop digital expertise and increase their online presence.**

3. Countries/private providers/NGOs must enhance **online confidential reporting mechanisms,** allowing anonymous reporting of THB cases as well as victims' self-identification. Chat, including chatbots, and instant messaging functions could be valuable online tools. Countries should work with private companies offering online services to **design out opportunities for traffickers,** develop **content analytics** to detect THB instances and set up easily accessible mechanisms for clients to **flag up** suspicious activities/advertisements. Where allowed by domestic legislation, this should be extended to companies offering online adult services. Online content and information (e.g., IP addresses) linked to flagged activities/advertisements should be stored securely by companies.

Actions to enhance investigation of technology-facilitated THB

4. Law enforcement should consider training officers specialised in both ICT and THB. Countries should also consider creating **technical support groups** staffed by sworn or non-sworn police officers with specialised ICT capabilities embedded within THB units. Furthermore, countries should review the design of the internal **distribution of digital investigative capabilities** to anticipate and avoid potential **bottlenecks in investigations.** As ICT-facilitated crime, including THB, is likely to continuously increase, the lack of specialist officers at the local level and the overreliance on assistance from (busy) centralised cyber-crime units are likely to create bottlenecks.

5. Law enforcement should make sure that **all officers** possess an adequate level of expertise in collecting and handling **electronic evidence**. Training on electronic evidence should be made integral to training curricula and constantly kept up-to-date due to the fast-changing technological and behavioural landscape. As the preservation of electronic evidence is key to building strong investigations, also **counsellors and NGOs first-respondents** need to be familiar with strategies to preserve digital evidence (e.g., by storing chat histories).

6. Countries/international organisations should regularly carry out a **strategic analysis** to generate knowledge on emerging trends on offenders' *modus operandi* as well as to keep uptodate with the fast-changing behavioural patterns of technology users and the technological landscape. Based on this strategic evidence, countries can then launch targeted police operations, set up cooperation agreements, as well as devise targeted awareness-raising campaigns. Knowledge should be regularly disseminated at the national and supra-national levels.

7. Countries should increase cross-border cooperation through **streamlined procedures**, the **sharing of best practices and technologies** (e.g., specialised software) and the enhanced **dissemination of practical information** about the contact points/dedicated units that serve as "privileged contact" in the case of THB cases, including ICT-facilitated THB. Cooperation and support between destination and origin countries should be encouraged (e.g., expensive technological equipment might be affordable only to more affluent destination countries).

Actions to enhance prosecution of technology-facilitated THB

8. Prosecutors should be provided with specific **training** on technology-facilitated THB and the handling of electronic evidence as well as its presentation before a judge/jury. Countries should take measures to ensure that **prosecutors are familiar with procedures** to request electronic evidence from private companies as well as obtaining evidence and cooperation from other countries both within the EU legal framework (via Joint Investigation Teams and European Investigation Orders) and outside the EU legal framework.

Actions to enhance cooperation with private companies

9. Countries should develop **data-sharing procedures** with companies holding relevant data and consider developing **cooperation protocols** with private companies, including social network and gig-economy companies as well as rental platforms to foster the timely provision of information. Such protocols/procedures should clarify the legal requirements under which ICTs companies, ISPs and content hosts operate; designate a contact point within companies; and clarify the national agencies responsible for specific actions, e.g. requesting evidence or taking down THB-related content. Refusal to share evidence or take down THB-related content should be timely, explicit, and motivated.

Actions to enhance international cooperation

10. A **smoother process should be established for Mutual Legal Assistance Requests (MLAs)**, including clearer procedures, increased usage of enhanced networks of contact points, including EJN contact points, and requirements for MLAs to be clearly set out and discussed at the outset. Countries should ensure that their personnel are adequately trained to process MLAs, EIOs and other international tools. Countries and international organisations should develop **commonly agreed and accepted templates** underpinning cooperation processes with a view to ease communication, decrease administrative burdens and minimise mistakes in the requests. Countries should also develop the use of **secure forms of electronic communication** and promote their adoption to smoothen international cooperation.

Actions to enhance training

11. **Joint Training Activities (JTAs)** should be envisaged for countries that are systematically engaged in joint THB cases. Transnational knowledge exchange can be fostered through participation in international/regional training focused on specific aspects of investigating ICT-facilitated THB. Such training should include case studies and scenarios on ICT-facilitated THB. Training on ICT-facilitated THB and associated legal instruments should also be provided to prosecutors and judges.

12. NGOs should receive training on the latest developments in both technological and THB landscapes, including changes in recruitment strategies. NGOs should be in a position to exchange experiences on international best practices.

Actions to enhance legal instruments

13. Authorities should devise **common procedures for the rapid exchange of digital evidence with ISPs** and should **re-assess the length of data retention obligations** imposed on ISPs (current periods are too short considering the length of police investigations). Efforts should be made to adopt a **common framework** regarding data retention obligations and sharing of electronic evidence.

14. To leverage on the full potential offered by the **Cybercrime Convention**, countries should (a) complete the harmonisation of national legislations with the Convention; (b) widen and enhance the training on the possibilities offered by the Convention as not all State Parties are currently using the tools available to their full potential; (c) raise awareness on the broad scope of the procedural powers and tools for international cooperation of the Convention, particularly in relation to THB cases; and (d) swiftly implement the measures included in the Second Additional Protocol.

15. Countries should carefully assess the issue of where their **contact point** (as per the Cybercrime Convention) is located within the criminal justice system to avoid **bottlenecks**. With the increasingly central role played by ICTs and electronic evidence, such contact points will be under increasing pressure and will be quickly overwhelmed if not adequately staffed. Countries might wish to consider staffing such contact points with personnel possessing expertise in different crime types, including ICT-facilitated THB.

16. Countries outside Europe should be encouraged to **adopt key international legal tools**, such as the CoE Cybercrime Convention and the CoE Convention on Mutual Assistance in Criminal Matters, to smoothen and enhance international cooperation.

17. **Cooperation and synergies** should be increased between the monitoring mechanism of the Anti-Trafficking Convention (GRETA and Committee of the Parties) and T-CY, for example, in the form of exchange of views as well as the development of capacity-building activities focusing on both conventions.

Actions to prevent victimisation and re-victimisation

18. Private companies, working with the authorities and NGOs, should increase online **social advertising** to prevent victimisation and improve the detection of technology-facilitated THB. Countries should increase their efforts to inform individuals about their employment rights in a language they understand, in cooperation with NGOs and with companies that provide hosting services for job advertisements. The impact of campaigns should be routinely evaluated.

19. Countries, NGOs and private companies that provide online and ICT services should run initiatives to **raise awareness on technology-related risks, including how traffickers might exploit technology** and how potential exploitative situations might begin. Schools and educators should be made part of this effort as children and young adults are exposed to heightened risks. Countries and NGOs should work with private companies offering communication and messaging services to design into the system information/warnings on the **safe use of private channels of communications**.

20. NGOs should offer training on techniques of data protection and safe use of technology as part of **victims' protection and reintegration programmes.** Victims should not be cut out of technology with the effect of disempowering them.

Cross-cutting action

21. Countries should include a technology strategy in their **national action plans** for combating trafficking in human beings.

Annex 1 | Building an evidence base on online and ICT-facilitated THB: List of sources

The evidence base has been built on the basis of a wide background research covering a variety of sources including: (a) international organisations; (b) academia; (c) selected national rapporteurs; (d) NGOs and charities; (e) private sector. A total of 62 outputs have been identified as relevant for the purpose of this work. While the outputs considered span the period 2003 – 2020, the vast majority was published from 2015 onwards, and 22 were published in the last three years. All the outputs considered are written in English (with one exception: the French version of a report produced by Myria, the Belgian '*Centre fédéral Migration*').

International and national organisations

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

Academia

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.

NGOs/charities/private sector

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.

Websites

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)

Annex 2 | Questionnaire for States Parties

Part 1. Impact of ICTs on THB

1. Based on evidence from your country, could you provide examples of the ways in which ICTs are used by offenders in the context of THB for sexual exploitation? (For each example, please provide details on the modus operandi of traffickers and the type of technology used, e.g. Internet, specific Websites, social media, Apps).

2. Similarly, could you provide examples of the ways in which ICTs are used by offenders in the context of THB for labour exploitation? (For each example, please provide details on the modus operandi of traffickers, the type of technology used, e.g. Internet, specific Websites, social media, Apps, *and* the economic sector in which exploitation takes place).

3. What are the emerging trends in your country in relation to the use of ICTs in THB (new types of technology, new modus operandi, new types of exploitation…)? Have you identified emerging online practices that may increase the risk of becoming victim of THB (both for sexual and labour exploitation)?

4. Does the DarkWeb play any role in THB in your country? If it does, could you please offer some details? (By DarkWeb we mean Internet pages that are only accessible through anonymising browsers, such as Tor).

5. In your country, are ICTs used to facilitate financial flows in the context of THB? If so, in what ways? To what extent are cryptocurrencies or cryptowallets used?

6. Overall, on a scale from 1 to 5, how would you judge the impact of ICTs on THB in your country?

1	**2**	**3**	**4**	**5**
Very limited				Very important

Part 2. Key challenges faced by State Parties in detecting, investigating and prosecuting ICT-facilitated THB

Detection

7. What are the strategies adopted by your country to detect online cases of THB?

8. More generally, what are the challenges in detecting ICT-facilitated THB?

9. Do you have any examples of best practices in detecting ICT-facilitated THB cases?

10. What type of training do you provide to investigators and other criminal justice actors in identifying cases of ICT-facilitated THB? What additional training could be offered to increase the effectiveness of detection strategies? How can the online identification of victims be strengthened?

Investigations

11. Thinking of **investigations into ICT-facilitated THB**, how much of a problem would you consider the following to be:

	Normally not a problem	A minor problem	A major problem
Data encryption			
Lack of technical knowledge among law enforcement			
High volume of data resulting in time-consuming investigations			
Speed of technological change (new technology appearing fast, etc.)			
Lack of technical equipment			
Lack of assistance from private sector			
Inadequate legislative tools, including mutual legal assistance tools			

12. For each problem that you consider 'major', please provide some examples and describe the steps, if any, already taken to overcome/mitigate it. For each 'major' problem, what solutions could be envisaged to overcome it?

13. Are there additional problems not listed in the table? (For each additional problem, please provide details on the problem and the solutions that could be envisaged to overcome it).

14. What do you consider to be the best strategies to conduct effective investigations into ICT-facilitated THB?

15. What training is currently provided to law enforcement in relation to investigations into ICT-facilitated THB? What additional training needs of law enforcement have you identified in relation to ICT-facilitated THB? Are there examples of training practices that you view as particularly successful?

Prosecution

16. Thinking about **prosecutions into ICT-facilitated THB specifically**, how much of a problem would you consider the following to be:

	Normally not a problem	A minor problem	A major problem
Attribution of jurisdiction			
Extradition of suspects			
Obtaining evidence from other countries			
Assistance from private sector			
Inadequate legislative tools, including mutual legal assistance tools			
Lack of training among prosecutors			

17. For each problem that you consider 'major', please provide some examples and describe the steps, if any, already taken to overcome/mitigate it. For each 'major' problem, what solutions could be envisaged to overcome it?

18. Are there additional problems not listed in the table? (For each additional problem, please provide details on the problem and the solutions that could be envisaged to overcome it).

19. What training is currently provided to prosecutors and judges in relation to ICT-facilitated THB? What additional training needs of prosecutors and judges have you identified in relation to ICT-facilitated THB? Are there examples of training practices that you view as particularly successful?

20. Does your country have specialised units within law enforcement and the judiciary tasked with handling THB cases with a large technological component (e.g., electronic and online evidence)? If yes, please describe their practices.

International Cooperation

21. What are the challenges of transnational investigations and judicial cooperation in the context of ICT-facilitated THB? What are the main obstacles to effectiveness, if any, and how these could be overcome?

22. Are there examples of good practices to enhance international cooperation?

Part 3. Existing tools to help prevent and combat ICT-facilitated THB

23. Can you please describe the most relevant domestic legal instruments used in combating ICT-facilitated THB? Is your legislation able to keep up with technological changes? If yes, how do you adapt to those changes? If no, how can it be improved?

24. Can you please describe the most relevant international legal instruments used in combating ICT-facilitated THB? Do you consider the existing instruments adequate? In what ways can they be improved?

25. Are there any specific gaps in the current domestic or international legislation that hinder the fight against ICT-facilitated THB?

26. Do you have any mechanisms aimed at preventing the use of ICT for THB purposes, including on social media and in relation to online job advertisements? If yes, please describe the practices in place and indicate the state authority responsible for their implementation.

Part 4. Leveraging on Technology

27. What technological tools, if any, are currently available in your country to identify victims of THB? Are artificial intelligence, facial recognition and/or big data analytics used to identify victims? Do you have a set of indicators ('red flags') to identify victims?

28. What technology-based initiatives exist in your country to assist victims and disseminate information to at-risk communities?

29. What technology-based initiatives exist in your country to support investigations and enhance prosecution?

Part 5. Cooperation with private companies

30. In what ways do ICT companies, including Internet host providers, social media and other online platforms, assist with the identification and removal of THB-related Internet content? How is filtering carried out? Is the current mechanism for filtering and removal effective? If not, how can it be strengthened? Can you provide some examples of good practices?

31. Are there requirements in your legal framework for filtering and removal of THB-related Internet content, and what are the sanctions for non-compliance? Is there a code of conduct for providers? Is the legal framework effective? If not, how can it be strengthened?

32. What are the obstacles faced by your country in working with ICT companies and Internet service providers, including content hosts and social media, in tackling THB? How can an effective partnership with ICT companies be built? What tools – both legal and operational – could help strengthen cooperation with ICT companies?

33. In what ways do ICT companies combat THB-related financial transactions? How can cooperation be strengthened in this domain?

34. Does your country have an independent body/regulator in charge of monitoring internet content? If yes, on what basis is such activity exercised? If not, in what ways is monitoring exercised?

Part 6. Cybercrime Convention (Budapest Convention)

35. In what ways, if any, does your country utilize provisions from the CoE Cybercrime Convention (Budapest Convention) to fight THB? If not, why is that the case?

36. Are there ways in which the Cybercrime Convention (Budapest Convention) and its Additional Protocols could be further used to fight THB?

Part 7. Protection of Human Rights

37. What measures are in place to protect human and civil rights of individuals, including data and privacy rights, when combating ICT-facilitated THB? If technological tools are used, for instance to sift through the Internet, what protocols are in place to ensure that such tools are protective of sensitive data, including on sexual orientation, religion and political views?

38. Do you have gender-sensitive protocols linked to the use of technology to combat THB? Do you have age-sensitive protocols? If so, could you please describe these protocols?

39. How is the confidentiality of data protected when sharing information between law enforcement and third parties, including private companies and charities? How is the victims' need for confidentiality in accessing services balanced against the need to collect evidence and information to assist the fight against THB?

Finally, is there anything else not covered in this questionnaire that you consider relevant in the context of combating ICT-facilitated THB?

Further materials

Could you please share with us any relevant non-confidential materials, including statistical data, press releases, summaries of police operations, that relate to ICT-facilitated THB, including:

- Use of ICTs in THB;
- Challenges in detecting ICT-facilitated THB, including identification of victims;
- Challenges in investigating and prosecuting ICT-facilitated THB;
- Cross-country cooperation in the context of ICT-facilitated THB;
- Cooperation with ICT companies;
- Tools to combat ICT-facilitated THB (legal and/or operational tools)
- Technology-based initiatives to combat THB;
- Examples of good practices

If your national rapporteur has explored the issue of ICT-facilitated THB, please share with us the relevant reports/materials.

Annex 3 | Questionnaire for NGOs

This questionnaire seeks to understand the impact of technology on trafficking in human beings (THB) based on evidence from your work in the field. By technology, we mean the broad set of information and communication technologies (ICTs) that allow users to exchange digital information. Examples of these are the Internet, online social media, and Apps for mobile phones.

Part 1. The impact of technology on THB

1. Based on evidence from your work, could you provide examples of the ways in which technology (ICTs) is used by offenders in the context of THB for sexual, labour or other types of exploitation? (For each example, please provide details on the type of exploitation and the technology used, e.g. Internet, specific Websites, social media, Apps).

2. Have you identified emerging online practices that may increase the risk of becoming victim of THB?

3. What are the challenges in detecting technology-facilitated THB? How can the identification of victims be strengthened?

4. Do you have any examples of good practices that you have developed in detecting technology-facilitated THB cases, and identifying victims?

5. Do you cooperate with law enforcement agencies in tackling technology-facilitated THB? What are the obstacles to such cooperation, and how could these be overcome?

6. What type of training, if any, do you provide to staff and volunteers in relation to the impact of technology on THB? What additional training could be helpful to increase the effectiveness of detection strategies? Do you have a team within your organisation specialised in technology-facilitated THB?

7. Are there any specific gaps in the current domestic or international legislation that hinder the fight against technology-facilitated THB?

Part 2. Using technology to fight THB

8. What technological tools, if any, are currently available to assist you in identifying victims of THB (e.g., specific Apps, big data analytics, Web crawling)? Do you have a set of indicators ('red flags') to identify potential victims? What type of technological tools would be helpful to have?

9. What technology-based initiatives, if any, are available to you to assist victims and disseminate information to at-risk communities? What technology-based initiatives would be helpful to develop?

10. Have you run any awareness campaign focused on the use of technology in THB? If so, could you provide some details of such campaigns?

11. Do you have gender-sensitive protocols linked to the use of technology to combat THB? Do you have age-sensitive protocols? If so, could you please describe these protocols?

12. How is the confidentiality of data protected when sharing information with law enforcement? How is the victims' need for confidentiality in accessing services balanced against the need to collect evidence to assist the fight against THB?

13. Based on evidence from your work, how would you judge the impact of technology on THB on a scale from 1 to 5?

1	**2**	**3**	**4**	**5**
Very limited				Very important

Finally, is there anything else not covered in this questionnaire that you consider relevant in the context of combating ICT-facilitated THB?

Further materials

If possible, could you please share with us any relevant materials you might have produced, including statistical data, press releases and reports, that relate to ICT-facilitated THB.

Annex 4 | Questionnaire for tech companies

This questionnaire seeks to understand the impact of technology on trafficking in human beings (THB) based on evidence from your work in the field. By technology, we mean the broad set of information and communication technologies (ICTs) that allow users to exchange digital information. Examples of these are the Internet, online social media, and Apps for mobile phones.

Part 1. Impact of ICTs on THB

1. Based on evidence from your company/sector, could you please describe the ways in which ICTs are misused by offenders in the context of THB (for sexual, labour or other types of exploitation)?

2. Have you identified emerging online practices that may increase the risk of becoming victim of THB?

3. What mechanisms have been developed by your company, or your sector more generally, to prevent the misuse of ICTs for THB purposes?

Part 2. Cooperation with law enforcement agencies and civil society

4. In what ways, if any, does your company cooperate with law enforcement agencies to facilitate the identification of victims and the investigations into ICT-facilitated THB?

5. What are the main obstacles to cooperation with law enforcement agencies in the context of ICT-facilitated THB?

6. Are there examples of good practices to enhance cooperation with law enforcement agencies?

7. What are the legal requirements that your company is subject to in the context of combatting THB?

8. What tools – both legal and operational – could help strengthen cooperation with law enforcement agencies?

9. In what ways, if any, does your company cooperate with civil society to facilitate the identification and assistance of THB victims?

Part 3. Leveraging on technology

10. What technological tools, if any, are currently available to your company to identify victims of THB? Are artificial intelligence, facial recognition and/or big data analytics used to identify victims? Do you have a set of indicators ('red flags')?

11. What technology-based initiatives exist in your sector to support investigations and enhance prosecution?

12. What measures are in place to protect human and civil rights of individuals, including data and privacy rights, when combating ICT-facilitated THB? If technological tools are used, for instance to sift through the Internet, what protocols are in place to ensure that such tools are protective of sensitive data, including on sexual orientation, religion and political views? Do you have age-sensitive protocols in place?

13. What type of training, if any, do you provide to staff in relation to the impact of technology on THB? What additional training could help increase the effectiveness of anti-trafficking strategies?

Finally, is there anything else not covered in this questionnaire that you consider relevant in the context of combating ICT-facilitated THB?

Further materials

If possible, please share with us any relevant non-confidential materials, including statistical data, press releases and reports, that relate to ICT-facilitated THB.

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE