Online and technology-facilitated trafficking in human beings

Summary and recommendations

GRETA

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

Summary and recommendations

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

March 2022

Council of Europe

The opinions expressed in this work are the responsibility of the author and do not necessary reflect the official policy of the Council of Europe.

The reproduction of the extracts (up to 500 words) is authorised, except for the commercial purposes as long as the integrity of the text is preserved, the excerpt is not used out of context, does not provide incomplete information or does not otherwise mislead the reader as to the nature, scope or content of the text. The source text must always be acknowledged as follows "© Council of Europe, year of the publication".

All other requests concerning the reproduction/translation of all part of the document, should be addressed to the Directorate of Communications, Council of Europe (F-67075 Strasbourg Cedex or publishing@coe.int).

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.

© Council of Europe, March 2022
Printed at the Council of Europe

Table of contents

Introduction 5

Summary of the report 7

The impact of technology on trafficking in human beings 7

Challenges in detecting, investigating and prosecuting technology-facilitated THB 10

Strategies and good practices 15

Training: what is provided, what is needed 20

Legal instruments 22

Human rights, ethics and data protection 25

Recommendations 27

Actions to enhance detection of technology-facilitated THB cases 27

Actions to enhance investigation of technology-facilitated THB 28

Actions to enhance prosecution of technology-facilitated THB 29

Actions to enhance cooperation with private companies 29

Actions to enhance international cooperation 29

Actions to enhance training 29

Actions to enhance legal instruments 30

Actions to prevent victimisation and re-victimisation 30

Cross-cutting action 31

Annex 1 | Building an evidence base on online and ICT-facilitated THB: List of sources 32

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.

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 Knowldge 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)