



DISRUPT MANUAL

on the use of digital evidence in
combating child trafficking

Disclaimer

This document contains material, which is under copyright of individual or several DISRUPT consortium parties, and no copying or distributing, in any form or by any means, is allowed without the prior written agreement of the owner of the property rights.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the DISRUPT consortium as a whole, nor individual parties of the DISRUPT consortium warrant that the information contained in this document is suitable for use, nor that the use of the information is free from risk and accepts no liability for loss or damage suffered by any person using this information.

This document reflects only the authors' view. The European Community is not liable for any use that may be made of the information contained herein.

© 2024 Participants in the DISRUPT Project

TABLE OF CONTENT

List of acronyms	7
Foreword	8
1. Introduction to Human Trafficking	8
1.2 Labour Exploitation	13
1.3 Forced criminal activities.....	14
1.4 Current Dynamics of Human Trafficking	15
1.5 Profile of perpetrators.....	17
2 Vulnerabilities of children and young people	18
2.2 Vulnerabilities related to the victim’s background and circumstances	18
2.3 Young age and limited knowledge of risks associated with online interactions.....	21
2.4 Accessibility of social media platforms	21
2.5 Profile of Child Traffickers	26
2.6 Ability to blend in	27
3 Technology use in child trafficking	28
3.1 Discovery	28
3.2 Recruitment.....	28
3.3 The manipulation of gender in recruitment.....	35
4 Modus operandi online	35
4.1 Common modus operandi for online sexual exploitation.....	37
4.2 Common modus operandi for recruitment towards child trafficking on gaming platforms:	38
5 Digital investigations in child trafficking: opportunities and limitations	39
5.1 General limitations of digital investigations.....	39

5.2	Challenges to identification.....	41
5.3	Collecting and analysing open-source information.....	42
5.4	Indicators of trafficking for sexual exploitation in online escort ads.....	43
5.5	Indicators for mainstream social media content:	47
5.6	Undercover operations	50
5.7	Hacking.....	52
5.8	Digital forensics	52
5.9	Extracting digital evidence	55
5.10	Recovering deleted data	57
5.11	Promising practices identified in improving public-private exchange of information in digital investigations.....	58
5.12	Use of AI in digital investigations	60
6	Use of digital evidence in prosecution & judicial response	68
6.1	Challenges to investigation and prosecution	68
6.2	Interpretation of emojis in court proceedings	70
7	Legal framework related to the collection, analysis and preservation of digital evidence	71
7.1	Guidelines on cross-border cooperation procedures in terms of collection and exchange of digital evidence	82
7.2	Challenges	90
7.3	Ethical Consideration in Collecting Electronic Evidence	90
8	Public-Private Partnerships in Combating Trafficking in Human Beings (THB)	93
8.1	General description	93
8.2	Promising Practices of Public-Private Partnerships: Case Studies	95
9	Child-Oriented Justice in Cases of Trafficking in Human Beings (THB).....	101

10	Using a victim-centric approach from investigation to prosecution	104
10.1	Understanding the importance of working with victims	104
10.2	Fostering a victim-centric approach.....	106
11	The Aftermath of Crime: Impact and Needs of Victims	107
11.1	Impact of Crime on Victims & Society	107
11.2	Needs of Victims in the Aftermath of Crime	111
11.3	Barriers to accessing needs and rights	116
12	Engaging effectively with victims of crime: a guide for practitioners	117
12.1	Building trust and rapport	118
12.2	Safety, privacy and transparency	125
12.3	Empowerment and support	131
12.4	Compensation for Victims of Trafficking in Human Beings (THB).....	134
	Bibliography.....	137

List of acronyms

- ❖ Victim Support Europe – VSE
- ❖ United Nations – UN
- ❖ European Commission – EC
- ❖ European Union – EU
- ❖ Human trafficking – THB
- ❖ United Kingdom – UK
- ❖ Law Enforcement Agency – LEA
- ❖ Non-SQL” or “non-relational” databases, - NoSQL
- ❖ Open-Source Intelligence – OSINT
- ❖ Write-ahead logging – WAL
- ❖ Native Language Influence Detection – NLID
- ❖ Native Language Identification – NLI
- ❖ Linguistic Inquiry and Word Count – LIWC
- ❖ Human Intelligence – HUMINT
- ❖ Joint Investigation Teams- JIT
- ❖ European Production Orders- EPOs
- ❖ European Investigation Order- EIO
- ❖ Public-Private Partnerships- PPPs
- ❖ Multi-Agency Risk Assessment Conferences – MARACs
- ❖ Post-Traumatic Stress Disorder- PTSD

Foreword

This manual is intended for all stakeholders working in the field of preventing and combating child trafficking and how would like to learn more on how to improve their practices surrounding the collection, analysis and use of digital evidence. The manual includes 12 sections, each dealing with a separate dimension of child trafficking, from the profile of perpetrators, to modes of online recruitment, techniques of digital investigations to the legal framework surrounding digital evidence and recommendations on how to foster a victim-centric approach across all processes.

1. Introduction to Human Trafficking

Human trafficking is a grave crime characterised by coercion, fraud, and abuse to manipulate and exploit vulnerable individuals. This covert, criminal enterprise operates on a vast and sophisticated scale, driven by a combination of political, social, technological, and economic factors. With an estimated yearly revenue of US\$ 245 billion in illegal profits per year (ILO, 2024), human trafficking and modern slavery have evolved into one of the most profitable illegal sectors globally, ranking third after arms and drug trafficking.

Definition of human trafficking:

According to Article 4 of the Council of Europe Convention, trafficking in human beings consists in a combination of three components:

Action: *the recruitment, transportation, transfer, harbouring or receipt of persons*

Means: *by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person (this element is irrelevant when the victim is a child)*

Purpose: *for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs (Council of Europe, 2005)*

Trafficking in numbers:

- ❖ 10 093 registered victims of trafficking in human beings and 2 097 convicted traffickers were recorded in 2022 in the EU.
- ❖ 63 % of registered victims of trafficking are women or girls.
- ❖ 41.4 % of all trafficking cases deal with sexual exploitation, although the prevalence is the lowest in the 2008-2022 period.
- ❖ 41.1 % of cases are linked to exploitation by forced labour and services, reaching in 2022 its highest prevalence; organ removal and other exploitative purposes, including use for benefit fraud, criminal activities and forced begging, account for the remainder.

- ❖ The EU countries with the highest numbers of trafficking victims are Bulgaria, Romania, Hungary, Slovakia, Croatia, Latvia, Lithuania, and Czechia, while the main countries of origin for non-EU citizens are Nigeria, China, Moldova, and Pakistan (Eurostat, 2024),

Child trafficking:

Child trafficking is defined as the “recruitment, transportation, transfer, harbouring or receipt” of a child for the purpose of exploitation (United Nations Palermo Protocol)

Child trafficking affects children of all backgrounds and demographics. According to an IOM data set, approximately 57.4 per cent of child victims in 2021 were female and 42.6 per cent were male. Child victims of trafficking range from 0-17 years old; with the largest group (~46%) being 13-17 (IOM, 2023). Because of their age children are differently impacted by trafficking than adults, with the impact further compounded depending on gender, ability, or other diversity

characteristics. Analysis of court cases shows that children are subjected to physical or extreme violence by traffickers at a rate almost two times higher than adults (UNODC, 2022).

Child trafficking can take place within or through any region or country with different levels of organization and can be classified into two large groups: domestic sex trafficking and international sex trafficking (Greenbaum, 2018).

In the EU children represent between 15% and 22% of reported trafficking victims (Eurochild, 2024; EEAS, 2021), often trafficked for sexual exploitation, labour, or forced begging. Most victims of child trafficking identified within the EU are non-EU nationals (e.g., unaccompanied minors fleeing war or

poverty). They are recruited by traffickers, who promise them a better life in the EU. The main trafficking hubs are Southern Asia, the Maghreb, and western Africa (especially Nigeria).

In many cases, children are sold by their parents, who cannot support themselves or their child and sell them to a human trafficker who promises high wages in Europe (Europol, 2018).

Typology of human trafficking:

Reasons for human trafficking include:

Sexual exploitation - *victims are predominantly women and children.*

Forced labour - *victims primarily from developing countries, forced to work in labour-intensive jobs, or kept in domestic servitude.*

Forced criminal activities - *victims must carry out a range of illegal activities. Victims often have quotas and can face severe punishment if they don't meet them.*

Organ donation - *victims often see little to no compensation and face health risks (European Parliament, 2023)*

1.1 Sexual Exploitation

Sexual exploitation remains a pervasive issue across the EU, particularly in sectors such as prostitution, escort services, the pornography industry, and massage parlours, which often disguise exploitation within legitimate business operations.

Definition of sexual exploitation:

Sexual exploitation can be defined as:

any actual or attempted abuse of a position of vulnerability, differential power, or trust for sexual purposes, including but not limited to profiting monetarily, socially, or politically” from the exploitation (Gerassi, 2015)

It can include sex trafficking, pornography, prostitution, or stripping, along with other sexual activities for profit (Greenbaum, 2014). Child trafficking for sexual exploitation is often interlinked with other forms of sexual exploitation, such as the production of child sexual abuse material, exploitation of children in prostitution, sexual exploitation of children in the context of travel and tourism and some forms of child, early and forced marriage.

By comparison to the general criteria for human trafficking, for cases involving minors, there isn't a legal requirement to prove force, fraud, or coercion – as minors cannot legally consent to these activities.

Statistics reveal that sexual exploitation victims are predominantly female (87%), with women comprising 73% and girls 27% of this group. The countries with the highest numbers of female victims included Romania, the Netherlands, Germany, Austria, Italy, and Spain. However, the true extent of child trafficking for sexual exploitation is very difficult to estimate.

This is due to several reasons: (1) trafficking victims are less likely to be identified than international trafficking victims across borders (Brayley & Cockbain, 2014); (2) boys and gender/sexual minorities are less likely to be identified as a result of cultural factors such as gender roles and social expectations (Greenbaum, 2020). Therefore, when it comes to child trafficking for sexual exploitation it is very

important to employ a gender perspective, given that victimization experiences can vary significantly between boys and girls.

Child trafficking for sexual exploitation is increasingly being facilitated by technology, which is employed by traffickers to recruit and exploit their victims. Europol has reported a rise in "sex tours", where victims are transported between cities to meet clients, reflecting the growing sophistication of trafficking networks (Europol, 2023).

1.2 Labour Exploitation

Labour exploitation, **the second most prevalent form** of trafficking within the EU, is widespread in cash-intensive sectors such as agriculture, construction, food processing, hospitality, and domestic assistance.

The concept of "labour exploitation" in the context of human trafficking is defined as 'forced labour or services, slavery or practices similar to slavery, and servitude' (UN Palermo Protocol). EU Anti-Trafficking Directive specifically mentions begging as a form of 'forced labour or services'.

In the case of children, labour trafficking can occur concomitantly with trafficking for sexual exploitation (e.g., child marriage).

Forced begging is one of the most common forms of labour trafficking in children within the EU, whether domestic or across borders, with seasonal intensification in certain areas. Undocumented children and/or children on the move are often found in exploitative situations. Often, parents are directly involved in forcing children into begging (UNODC, 2022).

Boys are also exploited in seasonal agriculture and in the production and distribution of narcotics in various EU countries (e.g., France, Germany, Italy and the Netherlands). Other sectors where trafficking may occur due to the demand for cheap labour are textile, food production, entertainment and hospitality industries (UNODC, 2022).

Online recruitment has facilitated this exploitation, with traffickers collaborating with recruitment agencies and subcontractors to present a facade of legitimacy while evading detection.

The most vulnerable children groups include minors who migrate from one region to another, both internally and across borders, and children living in the streets (UNODC, 2022).

Male victims predominate in labour exploitation, accounting for 66% of cases, though the exploitation of women, particularly in domestic work and cleaning services, has seen an increase. Women and girls exploited in private households often remain invisible due to their isolation and the hidden nature of their work. Overall, women and girls comprise 63% of all registered trafficking victims within the EU, emphasising **the gendered dimension of the crime**. Additionally, there has been a notable increase in the share of male victims, from 23% in 2017–2018 to 33% in 2019–2020, indicating an evolving pattern in trafficking that increasingly affects men and boys (OSCE, 2021).

1.3 Forced criminal activities

Though less prevalent than trafficking for sexual exploitation or labour trafficking, the exploitation for the commission of illegal activities is increasing within the EU. Traffickers take advantage of their victims to force or compel them to engage in criminal conduct.

In Europe the victims of this form of trafficking in persons are predominantly children, mainly due to the fact that persons under a certain age (13-15 years old) cannot be held responsible for the criminal acts they carry out. Statistics from Central and South Eastern Europe indicate that out of all victims of trafficking under this category 22% were girls and 4% boys.

Most of the times the **victims may not be aware** they are being exploited. Moreover, due to the complexity of the circumstances surrounding this type of exploitation, it is one of **the least identified forms of trafficking** at global level (UNODC, 2022).

The main criminal activities which children are forced to commit range from pickpocketing, theft and robbery to metal scrapping, drug dealing and drug transportation.

1.4 Current Dynamics of Human Trafficking

Human trafficking (THB) typically unfolds in a series of stages, each employing specific tactics to manipulate, control, and exploit victims. This process begins with the recruitment phase, commonly conducted in victims' origin countries, where traffickers use deceptive methods to entice individuals. Recruiters, often with local ties and shared cultural backgrounds, exploit various channels—such as the internet, employment agencies, media advertisements, and personal networks—to lure potential victims. By promising opportunities for better employment, education, or an improved future, they mask the grim reality of exploitation awaiting the victims.

The next stage, transportation, involves moving victims across borders to their eventual sites of exploitation. Traffickers use fraudulent travel documents, including fake passports and visas, to evade detection at immigration checkpoints. Victims, believing in the false promises given to them, remain unaware of the true nature of their journey, thinking they are headed toward legitimate prospects.

During this phase, traffickers often confiscate victims' identification documents to prevent them from seeking help or escaping, ensuring control. Transporters, who receive payment upon delivering victims to handlers, are crucial for sustaining the trafficking flow and ensuring traffickers' continued operations.

Upon arrival in the destination country, victims are forced into the exploitation phase, where they endure abuse and coercion. This exploitation can take multiple forms: forced labour, sexual exploitation, coerced criminal activities, forced begging, or even organ trafficking. Victims are subjected to severe physical and psychological abuse, including threats, violence, and intimidation, to maintain control and compliance. In cases of sexual exploitation, victims are confined to brothels, massage parlours, or private residences, forced into providing sexual services. In forced labour, victims work in extreme conditions across industries like agriculture, construction, domestic service, and manufacturing, often receiving little to no pay.

The digital age has introduced new complexities to human trafficking, making it easier for traffickers to recruit, control, and exploit victims. Digital recruitment has become increasingly prevalent, with traffickers leveraging social media, dating apps, and job boards to locate and lure vulnerable individuals. These platforms provide a veneer of legitimacy that helps traffickers establish trust and manipulate potential victims. Encrypted messaging apps and the dark web facilitate secure, hidden communications between traffickers and victims, further complicating law enforcement efforts.

Once victims are under their control, traffickers continue using digital tools for exploitation. Online platforms advertise and promote trafficked individuals, with escort websites and social media accounts openly soliciting clients for sexual services. This shift to digital platforms allows traffickers to operate discreetly, reducing their exposure to detection. Victims are often forced to perform online sexual services or are advertised on escort websites, complicating identification and rescue efforts.

Additionally, traffickers rely on technology to organize logistics, process payments, and maintain communications, embedding victims deeper within their trafficking networks and making intervention increasingly difficult.

1.5 Profile of perpetrators

Perpetrators of child trafficking for sexual exploitation may display multiple motivations, such as financial gain, where children are trafficked in exchange for money, drugs or other items of value; but they may also engage in sexual assault, rape, record images and videos of the child's sexual exploitation to control and/or to advertise them.

Research carried out in the US has shown that many child traffickers met the criteria for psychopathy, displaying a cluster of personality traits and behaviours which include superficial charm, manipulation, parasitic lifestyle, and a lack of empathy.

"I looked for girls who were willing to travel and [who were] running away from something or someone." – Child sex trafficking facilitator

Perpetrators of child trafficking are often calculating and predatory in their identification and recruitment of victims and they engage in deliberate acts of emotional and/or physical violence to control them.

When it comes to criminal background, research has shown that they usually possess diverse criminal histories, not necessarily linked to sex-related crimes (US Department of Justice, 2022).

Family trafficking

Trafficking of children by members of their own families is quite a frequent phenomenon and difficult to detect. This is due to the fact that victims would present what may look like an-age-appropriate life pattern: go to school, get good grades, participate in normal activities. They would also be reluctant to share their predicament with outside adults. Child victims are even more reluctant to disclose their exploitation when the perpetrators are family members, with whom they may share a bond of affection or from whom they would be materially-dependent.

Trafficking by organised crime groups

This type of trafficking also poses unique problems due to the fact that often minors are both victims and perpetrators of other crimes (e.g., drug trafficking). During their exploitation, the victims may be asked to carry out crimes in their turn, which they do not refuse due to being under coercion or due to trauma bonding.

2 Vulnerabilities of children and young people

2.2 Vulnerabilities related to the victim's background and circumstances

Research has shown links between risk factors for trafficking of children and forms of marginalisation, including social class, gender identity, sexual orientation and race. These elements may result in children and young people being excluded from the 'social mainstream' and thus heighten their exposure to perpetrators (Buller et al., 2020).

In addition to these there are, however, four categories, which place them at a higher risk for trafficking for sexual exploitation, namely (a) children in residential care; (b) children with disabilities; (c) unregistered children and (d) children belonging to LGBTQI+ minorities.

Children with disabilities:

- ❖ Particularly those with intellectual and mental disabilities may have a limited understanding of social cues and social interactions, leaving them more vulnerable to grooming and sexual exploitation.
- ❖ They may not consider themselves as victims as they may not be aware the actions they are asked to perform are against the law.
- ❖ Reports made by children with disabilities were not taken seriously by adults, due to their disability.

Children in residential care

- ❖ They have an increased risk of being sexually exploited in a number of ways including in the commercial sex trade.
- ❖ Because they are subjected to multiple placements their capacities to develop trusting relationships is limited and in turn, their abilities to differentiate sexual acts or demands and love (Roache and McSherry (2021).
- ❖ They are reported as 'going missing' more frequently than children living at home or in other care arrangements which in turn further heightens their risk of sexual exploitation (Canning et al, 2023).

Unregistered children

- ❖ They are often from marginalised communities, such as Roma in Bulgaria, Montenegro, and Romania, or disadvantaged social groups and ethnic minorities in Georgia.
- ❖ The lack of birth registration is prevalent among children born outside health facilities in Albania and occasionally among Albanian and Bulgarian children born abroad.
- ❖ Unregistered children, particularly those in residential or closed-type institutions are highly vulnerable, especially when they are forced to leave institutional care very early (e.g., at 15 in Albania).
- ❖ The recent surge in unaccompanied and separated children arriving in Europe has created another highly vulnerable group as these children are particularly vulnerable to trafficking due to their unregistered status and their reluctance to engage with authorities for fear of being deported.

Children belonging to sexual LGBTQI+ minorities

- ❖ They can be marginalised by their own family and community (including thrown out of the house);
- ❖ When they start going missing, relatives may offer law enforcement information that does not match the actual individual (e.g., a different gender and name).

- ❖ They may demonstrate riskier behaviours towards people they meet online due to their isolation and need for community.

Example of exploitation of a LGBTQI+ minor

A young boy from a conservative family is marginalized by his community once he comes out as gay. He is then groomed online by an older man who offers to find him work and help him in continuing his education. The perpetrator presents himself as a massage therapist and he pushes the victim into providing erotic massages. In this context, the perpetrator takes photos of the minor and uses them to advertise him online to get more clients. The perpetrator planned in trafficking the minor in the context of large sports events.

2.3 Young age and limited knowledge of risks associated with online interactions

Children have started using the Internet from a very young age, without being aware of the many risks associated with online interactions. In 2019, 4,000 children between the ages of eight and thirteen were found to be speaking to strangers online, with 43% of them speaking to strangers every day or at least once a week (E.I.E., 2021). Children and young people are particularly vulnerable to traffickers because they search for acceptance, attention or friendship (UNODC, 2020).

A Pew Research Centre report has shown that more than 33% of parents allowed their children to interact with a smartphone before age 5, and about 20% of parents allow children age 11 and younger to have their own smartphone. Moreover, 79% of children had phones before age 15 (Levine, 2022).

2.4 Accessibility of social media platforms

Most social media platforms are convenient and easily accessible for teenagers and adults, which creates a unique opportunity for traffickers to identify and initiate a relationship with their potential

victims. While the trafficking modus operandi on social media platforms has some common traits, there are also notable platform specificities, such as the ones identified below.

- ❖ Facebook, Instagram
- ❖ YouTube
- ❖ Reddit
- ❖ Discord
- ❖ Online gaming platforms, such as Roblox, Fortnite, Roblox Minecraft, and Gacha Life
- ❖ TikTok
- ❖ Skout.com/ MeetMe.com, LiveMe
- ❖ Snapchat,
- ❖ MyLOL,
- ❖ Periscope,
- ❖ YouNow,
- ❖ Tumblr,
- ❖ Kik,
- ❖ Omegle,
- ❖ Yubo etc.

Snapchat

A very popular app used by children and teenagers that allows the user to send a picture, text, or video to another Snapchat user. Snapchat is unique because it allows the sender to assign a duration to the message, up to 10 seconds. The danger with Snapchat is that it can be sent to anyone, and the sender believes that they can send a "snap" without being worried about any

ramifications of sending an inappropriate image or video. Snapchat has the ability for the receiver of the snap to capture it in a screenshot or by using a secondary device to take a picture, which is why Snapchat is the number one sexting app (Cranford, 2018). Moreover, the age verification feature of Snapchat is very weak (no official document is required) and users do not have to explicitly add accounts over the age of 18 to still see recommendations for adults, thus fostering a climate where underage users would be vulnerable to interactions with unknown adults.

One-third of teen girls and 30% of teen boys interviewed in a survey reported being exposed to unwanted contact on Snapchat in 2022. Internal Snap surveys revealed that over half of Gen Z users or their friends had experienced catfishing, and many were victims of sextortion. Moreover, an internal investigation revealed that 70% of victims had not reported their abuse because they knew no action would be taken by Snap; and out of the 30% reported cases, none were addressed. Snapchat raises potential risk also through its integration and/or connection to other apps such as YOLO (an anonymous messaging platform) and Hoop, which allows individuals to bypass safeguards on the Snapchat app and permitted strangers to connect with users on the platform.

Example of how Snapchat can facilitate child sexual exploitation & child trafficking

An undercover operation by the New Mexico Department of Justice using a decoy account for a 14-year-old girl with the username Sexy14Heather (“Heather”), initially listing her sign-up age as 18, but later modifying to a minor account showcased the lack of adequate safeguards on the platform. The platform not only enabled the account to search for other 15-year-olds on the app but even without adding any users, ‘Heather’ was able to receive friend requests from accounts identifying as a 15-year-old males requesting to exchange anonymous messages of Snapchat through a ngl.link. After the first single exchange and despite the privacy settings of the account, Snapchat proceeded to suggest 100+ other users to Heather, including adults seeking to exchange sexually explicit content as shown by their usernames like “naughtypics” and “gayhorny13yox”. (State of New Mexico vs. Snap inc., 2024)

Tinder

Tinder is a social media app used for dating; however, its primary objective is to facilitate hook-up. Tinder operates by using GPS location tracking to locate people (strangers) within a set range distance. Though Tinder was designed to be an adult-only social networking app, research has shown that it is also popular with young people, especially around the ages of 13-17 (Cranford, 2018). The main risk posed by Tinder is that the app makes it very easy for any child to start talking with a stranger, meet that stranger who could be an adult and be within walking distance of their home

Twitch

Twitch is a streaming platform, often associated with gamers which poses several risks related to personal information disclosure as well as possibility of providing financial rewards to different users. A study of 100 minor Twitch streamers showed that close to half provided their full names (47%) and stated their location 50% of the time. About 38% provided detailed schedules of when they would be live, and 64% linked and encouraged viewers to follow their other public social media. Viewers were able to donate money to 37% of streamers. Moreover, during live streams Twitch enables other users to enter live chats and engage with children, including asking them to perform explicit acts or share personal information. There is also a lack of efficient parental controls on Twitch, making restricting access to certain types of content very difficult.

Airbnb

Airbnb is mostly used for the exploitation part of human trafficking. For example, the concept of “pop-up brothels” have become more popular in recent years. A pop-up brothel is one that operates at a particular property, usually residential, for a short period of time. This type of modus-operandi enables criminals to move victims quickly from one location to another, making it difficult for law enforcement to locate and save them.

Online gaming platforms

Used by children and teens to play online, along or in teams. Games provide an opportunity for adults to interact with children & form relationships with them. They enable the gifting of items among users. Although games are public venues, their content is largely ephemeral in nature (e.g., chats via voice or text), making it difficult for authorities and/or parents to detect instances of grooming. While Roblox has parental controls, employs AI plus human-based moderation, and prohibits sexual content, children have still found ways to circumvent these controls such as using external platforms like Discord alongside Roblox to voice chat to other users free of filtering and to share links to user-created, hidden, sexually explicit, subgames known as 'condo games.

Example of how gaming platforms can facilitate child sexual exploitation & child trafficking

Roblox is an example of gaming platform which can be easily exploited for trafficking and or CSAM. An example of this are Condo-type games. The initial game (The Condo) had a setting which included a couple of rooms and a kitchenette, a pool in the backyard, thus resembling a condominium. Inside there were numerous Roblox avatars sported profanely exaggerated anatomies engaged in sexual acts, and the speech bubbles above their heads were full of swear words and slurs. Several other games have since been released, following a similar set-up (Haha, GAMEGAMEGAM, SCAR OF\$).

Discord groups are used to share links to new condo games and discuss while in the game. Thus users, take advantage of the fact that Discord does not prohibit linking to Roblox sex games, though they do require that adult content is limited to channels and servers explicitly marked for ages 18 and older.

Sugar daddy/Sugar baby websites

These are websites, where individuals connect with each other seeking relationships under a commercial arrangement, in which sexual activity is expected or implied in exchange for financial compensation. Though minors are theoretically excluded from such platforms, the age verification mechanisms are often weak thus enabling minors to access them pretending to be adults. In this context, the trafficking dimension may be difficult to prove due to the blurring of boundaries between the exchange of items of value in furtherance of so-called “dates”.

OnlyFans

While there is still limited evidence on the use of OnlyFans for the exploitation of minors, some preliminary studies seem to showcase connections between OnlyFans.com profiles and the darkweb (Anti Human Trafficking Initiative, 2022).

2.5 Profile of Child Traffickers

Irrespective of their individual profile, child traffickers can often be grouped in five categories (Network, 2018):

- Pretender
- Provider
- Promiser
- Protector, and
- Punisher



Fig. 1 – Typology of Child Traffickers

2.6 Ability to blend in

Research has shown that child traffickers are able to blend in society by using their status to gain access to children and dispel any suspicions. They often appear to both parents and children as someone that can be trusted.

3 Technology use in child trafficking

Technologies help perpetrators discover, recruit, coerce and control their victims.

3.1 Discovery

Social media platforms are used as 'virtual catalogues' to discover new victims. Moreover, the type of personal background information that is usually shared via these platforms (e.g., family relations, level of education, home address, list of friends, photos of daily life) enable traffickers to develop tailored-made grooming approaches. Thus, technology has given traffickers access to a more extensive potential victim pool than in the past, thus heightening the dangers and risks associated with sexual exploitation. A 2016 report by the National Centre for Missing and Exploited Children noted an 846% increase in reports of suspected child trafficking from 2010 to 2015, which arguably can be linked to the use of the Internet (De Bolle, 2020).

3.2 Recruitment

Perpetrators can recruit their victims without face-to-face communication, which decreases their chances of being identified by law enforcement agencies. Most if not all social media platforms have been identified as spaces for recruitment in all types of sex and labour trafficking, from older generic platforms such as MySpace and Facebook to newer platforms such as Instagram, Snapchat, Meetme.com, as well as messaging apps, such as WhatsApp and dating platforms, such as Plenty of Fish, Tinder and Grindr (Anthony, 2018).

Often interactions begin on mainstream platforms (e.g., Reddit) and are then moved to closed groups on more niche platforms (e.g., Discord) by traffickers. Moreover, traffickers exploit the way children

and young people themselves circumvent platform limitations (e.g., limitations related to no swearing, no sexual content etc), for example by sharing content via other parts of the gaming ecosystem—most notably Discord, which allows users to talk to one another via text, voice, and video, either one-on-one or in groups—they exploit the fact that Roblox’s enforcement mechanisms end at its own platform.

There are two main types of recruitment which most traffickers employ:

- ❖ Active recruitment (aka hunting) and;
- ❖ Passive recruitment (aka fishing).

Recruitment strategies	
Active	Passive
Proactive pursuit of victims (e.g., in online communities, gaming forums) and of potential buyers	Passive pursuit of victims (e.g., posting job advertisements online; creating fake employment agencies)
Trafficker initiates contacts based on victim’s characteristics (e.g., social circumstances, mental health etc.)	Victim is the one initiating contact by responding to an ad.
At onsite, relationship is friendly, and it gradually develops towards more toxic & aggressive forms.	The ads are aimed at attracting any number of victims interested in working in various industries (e.g., sex industry, hospitality, modelling).

Table 1 – Different recruitment strategies employed by traffickers

Active recruitment is less detectable as traffickers reach out (often via private messages) to different

individuals they have identified as being vulnerable (e.g., children who have a difficult relationship with their parents, children who feel lonely etc; teenagers seeking employment). Once contact is made, traffickers employ different tactics, as explained in the section above to gain the victim's trust and exert control over their behaviour. Victims typically only realize they are in an exploitative situation very late, when they have already provided the trafficker with significant resources (material and emotional) to make it very hard for them to escape the situation (Europol, 2020).

Passive recruitment is sometimes also called the 'hook fishing' technique, where traffickers proactively cast bait in the form of enticing but fraudulent job advertisements. These ads are posted on trusted job portals and social media marketplaces (e.g., Facebook marketplace), leveraging the credibility of these platforms to deceive potential victims. Criminal networks go to great lengths to create convincing facades, including setting up elaborate websites for fake employment agencies. These websites are often promoted on social media to reach a broader audience and may feature live chat functions to simulate immediate contact with hiring managers. The sophistication of these schemes can be remarkably high. The traffickers' ability to create realistic job offers and professional-looking websites makes it difficult for job seekers to discern the deceit. This passive approach is highly effective in drawing in victims, particularly those desperate for employment and willing to take risks for the promise of a better job abroad (Europol, 2020).

Within the two modes of recruitment, there are various tactics as shown below:

The 'lover boy' scam

It involves traffickers exploiting emotional vulnerabilities to recruit victims into forced prostitution. This method involves building a false romantic relationship, isolating the victim from their support network, and coercing them into prostitution. The approach preys on individuals facing economic hardship, using emotional manipulation and false promises to control them.

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 (Council of Europe, 2022 & Europol, 2024).

False Job Advertisements

In the realm of labour exploitation, technology facilitates recruitment through misleading job advertisements and online platforms. The shift from traditional to digital recruitment channels has been accelerated by the COVID-19 pandemic, with traffickers increasingly using social media and job search websites to lure victims. These platforms often host deceptive ads promising high wages and good working conditions, only for victims to discover substandard conditions upon arrival. The exploitation is often masked by the appearance of legitimacy, with traffickers mimicking legitimate businesses and using well-known job portals to attract victims.

Impersonation of Recruitment Agents

Traffickers sometimes assume the identity of reputable hiring companies or recruiting firms. They win the trust of possible victims by putting on a professional front. The abuse of this trust results in financial bondage when payments are collected for services like transportation or job placements that never happen. This financial trap makes sure that victims continue to work under abusive conditions to pay off their debts, keeping them under the traffickers' control.

Debt Bondage

The collection of recruitment or transportation fees can result in debt bondage, where victims are forced to work under abusive conditions to repay their debts. This form of exploitation effectively traps victims, making it difficult for them to escape their situation due to the financial obligations imposed upon them.

Recruitment by peers

It is important to remember that perpetrators are not always adults. Children can be recruited into child sex trafficking by their peers; by young adults who are both victims and intermediaries in the trafficking ring or by young traffickers pretending to be friends or romantic interests (US Justice Department, 2023).

Blackmailing is a commonly used strategy across different types of modus operandi and countries. This is often done by first collecting “compromising” information about the victims, for instance by asking for naked pictures or videos, and then using 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. 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).

The use of one or another social media platform is heavily reliant on the country; the mode of recruitment employed and the type of trafficking (see. Table 2).

		Facebook	Instagram	Snapchat	Chat apps (WeChat, WhatsApp)	Dating sites & apps	YouTube
Types of trafficking	Agriculture and Animal Husbandry	✓			✓		✓
	Arts, Sports and Entertainment	✓	✓				
	Bars & Strip clubs	✓	✓				✓
	Domestic work	✓			✓		
	Escort Services	✓	✓	✓	✓	✓	
	Illicit Massage Business	✓	✓		✓		
	Outdoor Solicitation	✓	✓	✓			
	Personal Sexual Servitude	✓	✓	✓	✓	✓	
	Pornography	✓	✓		✓		✓
	Remote Interactive Sexual Acts			✓	✓	✓	
	Restaurants & Food Service	✓			✓		
	Travelling Sales Crew	✓	✓	✓			✓

Table 2 – Links between Social Media Platforms and Types of Trafficking¹

¹ Adapted from B. Anthony (2018) "A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking", p 17

When it comes to online platforms, it can be very difficult to distinguish between recruitment for trafficking and legitimate interactions (e.g., real employment ads; profiles of independent sex workers). One reason for this is the effort traffickers invest in building credible profiles (e.g., image and video manipulation of visual content to alter age and appearance; adopting language patterns specific to younger age groups etc).

Example of how Reddit is exploited for online grooming

Subreddits dedicated to [i am lonely] [teens] [teenrelationships] [gaming] [hate my parents] [need a friend] are a very good recruitment area. Frequently under posts seemingly by young people/children expressing some type of physical and/or mental distress there are numerous users offering to follow up the conversation in private messages (DMs) and/or users sending invitations to private Discord groups, which are allegedly created solely for teens struggling with loneliness, mental health.

The same phenomenon can be encountered in advertising sexual content. OnlyFans accounts are often advertised on Snapchat and on Instagram, which are meant to give a small preview of what to expect behind the paywall and to create a strong audience base for the paid content.

Private chats are where most, if not, the most intelligence-relevant information appears. Once users are 'added' as friends on different platforms, they encourage underage individuals to communicate through private and often highly secure means (e.g. darkweb chat, encrypted messaging). A common goal of these conversations is 'sexploitation', whereby the child or teenagers is persuaded to send explicit pictures which are then used as leverage to potentially arrange physical meetings. The physical meetings are the most dangerous moments as they can enable physical harm, assault or kidnapping and can result in human or sex trafficking.

Links across platforms are common in all stages of child trafficking, from grooming to exploitation. Instagram accounts often act as ‘teasers’ for sexually explicit content, including links in their profile bios to other platforms such as Telegram channels, OnlyFans accounts where the actual videos are shared. Often the video shared on Telegram or Reddit are hosted on Terabox (a file sharing site).

3.3 The manipulation of gender in recruitment

Gender plays an important role in online grooming, especially for the purpose of gaining the trust of the victim. Thus, male perpetrators either work with female perpetrators to make their behaviour more trustful or they create fake online female personas (e.g., a sister, a female cousin) which are then used to vouch for their actions.

4 Modus operandi online

Online grooming of minors often follows a certain communication pattern, which can be used as a threat indicator. It is important to note that while researchers have identified different ‘stages’ within the grooming process, these do not always follow one another. Quite the contrary, often conversations evolve in a circular fashion, with perpetrators touching onto sexual (Stage 4) before returning again to trust building (Stage 2), in accordance with how persuaded they perceive the victim to be (Borg et al, 2023).

Stage 1 – Friendship forming (questions about profile exchange information)

- ❖ Exchanging email address/Messaging profiles;
- ❖ Asking the age/gender/location/name
- ❖ Personal information/Details about family

Stage 2 – Trust building

- ❖ Questions on favourite hobbies/activities
- ❖ Giving compliments;
- ❖ Exchanging photos;
- ❖ Building mutual trust;
- ❖ Showing feelings like anger/love.

Stage 3 – Risk assessment

- ❖ Questions on relationship with family & friends;
- ❖ Acknowledging wrongdoing;
- ❖ Questions to ascertain whether child is alone;
- ❖ Assessing the risk of conversations.

Stage 4 – Exclusivity

- ❖ Expressing feelings of love and exclusiveness;
- ❖ Moving conversations to more secure/private platforms/types of messaging.

Stage 5 - Sexual

- ❖ Conversations about body & intimate parts;
- ❖ Sexual content;
- ❖ Sexually oriented compliments;
- ❖ Providing body descriptions;
- ❖ Exchanging photos;
- ❖ Fantasy control and aggression.

Conclusion

- ❖ Arrange further contact and meeting

4.1 Common modus operandi for online sexual exploitation

- ❖ **An adult joins the social network to meet minors.** They may portray themselves as the same age or slightly older as the targeted minor.
- ❖ Often **individuals seek out new victims on mainstream social media platforms**, such as Instagram, YouTube or Reddit and then invite them to a private site to avoid moderation by the original platform.
- ❖ The **trafficker may use multiple false identities** on the same platform to exert increased peer pressure on a victim. They may even replay archived videos of past victims (called ‘loops’) that fool the current victim into believing that their sexual behaviour is normal for minors. After showing a video of the previous victim doing a sexual act, they would then “dare” victims to do something “wild,” a sexual act.
- ❖ **The adult forms a relationship with the victim** (see previous section on different types of trafficker profiles).
- ❖ Webcam sex is particularly dangerous because it can lead to transnational exploitation, as footage can be seen all around the world. Furthermore, this type of commercial sex often is carried out via livestream, thus making it easier for criminals to escape blockers and censors put in place by LEAs to detect child exploitation on the Internet. **Webcam sex is not usually recorded** so the probability that a digital footprint is left behind is highly unlikely (Barney, 2018).
- ❖ Another modus operandi is that of **‘new kid on the block’**, where traffickers pretend to be young children themselves that have just moved into the area. To support this story, they often ‘check in’ at a location nearby creating a false sense of trust.

- ❖ For offenders to fulfil their goal and make potential victims feel comfortable, **they will proactively offer nude images of their 'online persona'**. While real images might be used as well, the sexualization of harvested images of children seems to be more dominant at this stage, with use of face-swap software and AI-based deepfakes (Kietzmann et al., 2020), allowing offenders to create photorealistic imagery easily.
- ❖ Overlaying a child's naked body over multiple faces allows offenders to **create multiple proxy-identities for the parallel exploitation of different victims**. The over-abundance of children photos makes this stage much easier for the offenders (Kietzmann et al., 2020).

4.2 Common modus operandi for recruitment towards child trafficking on gaming platforms:

- ❖ **User 1 who is very good at playing a certain video game:** Looks for a child/young person who is playing a multiplayer game alone, too much, at odd hours, with a low rank. Asks the child to play and helps them win. Talks over chat focusing on learning the potential victim's schedule, likes and dislikes. Become a friend. Asks the potential victim to join a Discord server for other children/young people who play the game.
- ❖ **User 2 takes over and becomes a bad friend.** They also know how to play the game but not as well. They spend most of their time talking to the potential victim and making them feel like they are part of a group on the server. Find out from the first person what the potential victim likes, what their vulnerabilities and triggers are. Sends a photo of a sexual nature to the potential victim.
- ❖ **At this point the situation can present in different ways depending on the profile of the perpetrators.** They may use loops to show the potential victims sexual content produced by

other victims and dare them to do the same. Or blackmail/threaten them using personal information collected.

5 Digital investigations in child trafficking: opportunities and limitations

When it comes to digital investigations in child trafficking there are several types of actions that are employed, such as:

- Open-source intelligence
- Undercover operations in digital space
- Hacking
- Digital forensics

5.1 General limitations of digital investigations

Lack of authentication information

- ❖ Accounts are often unauthenticated.
- ❖ In the case of children-specific platforms, users are typically not asked to prove they are children. This is because of challenges posed by the introduction of age verification features when it comes to children, who would not have identification documents or credit cards to prove their age. It is therefore highly likely that anyone can sign up as a child on a service without any credentials, and these accounts are not authenticated to any identity.

End-to-end communication encryption

- ❖ Perpetrators make use of end-to-end encryption, allow connections from obfuscating proxies, and provide unattributable cloud storage

Complexity of online content

- ❖ In gaming platforms, it is difficult for investigators to observe all parts of the game at once (audio & text chat)
- ❖ Use of "imperfect" language forms online, such as the use of non-standard language and linguistic variability (Wybo et al., 2015).

Ephemeral character of content

- ❖ Web pages can change significantly over time. A page can be altered from the moment the message or post was initially made to when the investigator had access to it and attempted to make a copy. For example, a page can initially display the message "I will see you soon!" followed by a firearm emoji and then be altered to replace the firearm with a bouquet of roses.

Amount of information

- ❖ It can be difficult to identify relevant profiles, since not only can there be multiple profiles under the same name, but some delinquents use aliases to ensure anonymity

Legal limitations

- ❖ There are concerns about the legality of digital investigations and the efficiency of the legal safeguards put in place.

5.2 Challenges to identification

There are several challenges to victim identification which are linked to the modus operandi of child trafficking for sexual exploitation.

Trauma bond

Often child sex trafficking victims retain a sense of loyalty to their traffickers and may not see themselves as victims. This is due to complex trauma resulting from exposure to extreme coercion and emotional abuse. Trauma-related coping mechanisms can lead first-line practitioners to miss the signs of trafficking, and thus hinder or delay the identification of children as victims. This is particularly applicable for certain cultural groups due to implicit societal biases and the adultification of children from those cultural groups.

Gender bias

Male victims are less likely to be identified as victims of sex trafficking than females. This is due to multiple reasons, such as:

- They do not self-identify as a victim;
- Cultural norms prevent them from seeking help from first-line practitioners;
- Practitioners are less likely to look for male victims;
- They are less likely to be reported missing by their families, especially when they would have left their home/been kicked out by their families;
- They often interact differently with practitioners, which makes their testimony less credible (US Department of Justice, 2023).

5.3 Collecting and analysing open-source information

OSINT has been extensively used in collecting information on different types of crimes. In the case of child trafficking several uses can be identified:

- ❖ To monitor news media for information related to child trafficking incidents at local and international level, which may provide insights into the profile of the victims and suspects as well as the modus operandi being employed (e.g., modes of transport, how the victims were lured etc)
- ❖ To identify indicators of child trafficking across social media platforms and other types of websites
- ❖ To verify and complete intelligence collected from other sources.

Sources:

- Online media outlets
- Public discussion groups on different social media & gaming platforms
- Publicly accessible databases (e.g., business registration information)
- Escort websites

- Classified web pages for advertisement, referring to generic websites where individuals post advertisements or browse for items or services to buy or sell.

Example of DISCORD Search terms:

These are some commands (filters) used in the discord search bar to search things easier. to narrow down your search, use the following filters along with your search query.

- a. from: user --> Shows results from a specific user.*
 - b. mentions: user --> Shows anytime someone mentioned the specified user.*
 - c. has: link, embed or file --> Shows messages that contain specified element.*
 - d. before: date --> Results only show messages sent before specified date.*
 - e. during: date --> Results only show messages sent on specified date.*
 - f. after: date --> Results only show messages sent after specified date.*
 - g. in: channels --> Results only show messages sent in specified channel.*
-

5.4 Indicators of trafficking for sexual exploitation in online escort ads

According to a 2022 report prepared by the US National Institute of Justice and the Justice Research and Statistics Association the following set of indicators have been validated for detecting instances of trafficking in online escort ads². Though these indicators have been developed for online escort ads some of them may be useful also in the case of mainstream social media platforms (e.g., Instagram) used to advertise behind a paywall content (e.g., OnlyFans):

² It is important to remember that the data sample used was restricted to US-based content, however it is highly likely that many of these indicators would also appear in similar content for other geographical reasons.

Trustworthiness of provider

- ❖ Language assuring potential clients of provider trustworthiness was over four times as likely to indicate trafficking.
- ❖ For massage ads, this language was used in 20% more trafficking ads than non-trafficking ads.
- ❖ Traffickers use trustworthy language to foster a sense of confidence in the customer that the ad is a legitimate one, there is no coercion or risk of foul play.

Obscured Phone Number

- ❖ Obscuring the phone number is over 12 times more likely to indicate trafficking, provided other indicators are also present.
- ❖ This indicator does not apply however to massage ads, as in these cases the enterprise advertises itself as a legitimate one and therefore providing a contact number is a must.

Ethnicity of Provider

- ❖ When the ethnicity of the provider is indicated, the ad is over 5 times as likely to be associated with a trafficking case. This however does not apply in the case of massage ads.

Language suggesting youth

- ❖ This language increased the likelihood that a case was a trafficking case by over **four times**. However, this indicator needs to be applied with caution and in relation to others, due to the fact that non-trafficked sex workers may also use this type of language regularly as part of marketing strategies.

In addition to the above there are other indicators, which can be considered but which research findings identify as being less reliable.

Communication with buyers is carried out by a 3rd party (trafficker)

- ❖ In cases where the sex traffickers communicate directly with the buyers, there is a higher likelihood that the age of the victim is likely younger (under 13) (Van der Watt, 2023).

Age stated as 18

- ❖ This is not a reliable indicator for child trafficking as it is often used as a marketing strategy by both traffickers and non-trafficked sex workers (e.g. to imply a youthful appearance).

Other similar indicators that are frequently associated with both categories and can therefore only be considered in association with indicators from the first category are:

- ❖ Movement language ('new'; 'limited time');
- ❖ Control movement language (e.g. preference for a certain location);
- ❖ Restrictions/Preferences for Client Ethnicity
- ❖ Client Screening Language
- ❖ Payment language
- ❖ Multiple providers
- ❖ Available 24/7

In addition to the above, a special role is played by the use of emojis. By themselves, it would be very difficult to predict trafficking simply on the basis of emojis. This is because they are also used by non-trafficked sex workers to advertise their services (especially when these services are advertised on non-dedicated platforms, such as mainstream social media platforms). Emojis can be employed to describe money or the types of provider services (e.g. tongues, water drops, open or closed umbrellas). However, research has shown that emojis seem to occur in more cases of trafficking ads than non-

trafficking ads. There are also combinations of emojis which are often associated with trafficking (see section below on indicators for mainstream social media platforms).

Visual indicators

- ❖ obscured face (pixelation, placing an emoji, cropping the head), visible tattoo, hotel room, third party photo, professional photo) were not significant correlates of trafficking. This is also due to widespread photo manipulation, use of stolen or fake images and a general uniformity of styles and posing for adverts of sexual services.
- ❖ *'looking young'* is also not a reliable indicator due to the extensive use of photo filters in such adverts
- ❖ In the case of minors, they are often made to look older using cosmetics and other techniques (e.g. photo manipulation).
- ❖ It is important to note that foreign nationals are at a higher risk of being trafficked (Musto and Boyd 2014), so advertisements containing images of people of different races and ethnicities should be more heavily scrutinised, as this could be a possible indicator of exploitation (Dukes, 2020).

Overall, this reveals the importance of combining analysis of indicators in escort ads with other sources of evidence to make more definitive determinations of trafficking.

5.5 Indicators for mainstream social media content:

Instagram

Instagram is often used to advertise behind paywall content (e.g., OnlyFans accounts), but due to platform restrictions account holders must use different cover-up strategies in order to avoid the content being flagged as inappropriate.

General detection of adverts linked to sex work (which may be associated to child trafficking³):

- Age: age 18 or birth year 2006
- Size: height; bra size
- Ethnicity: in text: Asian or flags representing countries
- General description or username: Cutie/Sweet/Princess/Brat
- Occupation: student/in school
- Emotional status: Bored, looking for fun
- Text on reels: often the text indicates that certain words/letters must be replaced with others to get the full meaning
- Use of emojis:
 - References to virginity - emojis for cherries & cherry blossom
 - Young age – growing hearts, butterflies and fairy emojis.
 - Movement references – airplane emojis signifying ‘new in town’ or ‘need to travel to place where person is located’
 - Price: roses (number of roses may be an indicator of price)

³ As explained above some of these indicators have proven to be unreliable when considered independently in research on sex adverts.

- Trafficker: crowns (single and double crowns can indicate the presence of a trafficker and that they are the ones in control – the boss)

Reddit

One way of investigating Reddit is by identifying subreddits which make reference to child sex, child pornography, paedophilia. These can be used separately or in combination (Jane Doe vs. Reddit, 2021).

Jailbait	Dirty Small	Teen Beauties	Adorable porn	Snap leaks	Dirty snapchat	Nudist beach
Barely legal	Fauxbait	2000s girls	Funsized	Nude 18	Teen models	Pure nudism
Legal teens	Petite	Teen Pussy	Xsmall girls	Tiny tits	Preteen girls	Trapbait
18 NSFW	AA cups	Too cute for porn	Legal teens	College sluts	Chestybait	Assbait
18+ NSFQW	Small boobs	Innocently naughty	Young porn	Rate my nude body	Cute girls	Preteen boys
Hentai IRL	Down blouse	Gone wild	Young pretty hoes	Creepshots	Just teens	

Table 3 – Reddit lexicon linked to child sexual exploitation

It is important to remember that online indicators vary across languages

- ❖ In Chinese traffickers are using codewords for “escort” and “brothel” like: “Peripheral” (“外围”), which is based on the historical context that sex workers used to reside in the peripheral towns around the centre, and “Lou Feng” (“楼凤”), the ancient Chinese word for “brothels.”

“Loli” (“萝莉”) indicates the involvement of minors; They also use the nail painting emoji to indicate escort services.

- ❖ In Bangladesh, traffickers evade detection on social media by using codewords like “residential hotel” (“আবাসিক হোটেল”) to indicate compounds facilitating sex work.
- ❖ In Vietnam, the term ‘meo’ or ‘2k9’ is used to refer to underage female sex workers.

Snapchat

On Snapchat some of the terms employed, include:

- ❖ Pizza sellers – a proxy for child porn
- ❖ Trade young and trade girls
- ❖ Teen busy
- ❖ Rape baby

Considering the strong interactions between Snapchat and Reddit, the lexicon developed for one platform could be a good starting point for the other platform as well.

Example of covert online language

- ❖ Other methods employed by traffickers online are the use of esoteric language structure. For example: Have you got PTHC, where PTHC stands for Pre-Teen Hard Core. Moreover, to avoid detection the PTHC is further split in longer sentences to escape algorithmic detection on a keyword basis (e.g., Participate this coming Tuesday and don’t forget to Help those less fortunate this Christmas).

5.6 Undercover operations

Undercover operations, carried out by law enforcement, require them to engage in online interactions taking place on chat channels, online forums or by becoming ‘friends’ with the suspects or their friends on social media. This can be done using ‘sock puppets’ or by taking over another person’s account and then communicating with the suspect under someone else’s identity.

Good practices in creating sock-puppets

Adopt robust OPSEC procedures: *employ a password manager – to manage different accounts with strong passwords; use a burner phone with a prepaid SIM card; be careful about the WIFI networks you employ (never use personal ones); conceal IP address.*

Use an email service that looks legitimate (e.g., Gmail) and won’t raise any red flags by AI systems deployed by platforms to check for fake users.

Create a credible persona – using tools such as [FakeNameGenerator](#) ensuring that the name matches the target group; or for photos [This Person Does Not Exist](#). When using AI generated photos make sure to zoom in closely to check for flaws and remedy them. It is also important to consider gender dynamics in your choice of sock-puppet and to ensure that you cultivate a distinct personality trait for your persona to help with credibility. Make sure that your login patterns emulate the behavioural patterns of your persona.

Establish an actual social history across different platforms

Employ a long-term approach to using sock-puppets & make sure to age your accounts before using them for operational purposes.

Undercover operations also have their limits, such as:

- ❖ **Resources** - police officers can engage with only one suspect at a time. To address this limitation some organisations, have set-up initiatives aimed at developing automated chatbots which can interact with online users (e.g., Sweetie).

- ❖ **Operational feasibility** – the quality of avatars/bots needs to be very good by comparison to when they were first launched to prevent them from being easily identified by perpetrators.
- ❖ **Legal concerns** - when it comes to the legality of unilateral extraterritorial online undercover operations. Especially in cases where the undercover agents commit authorised crimes, some states may perceive this as a violation of their territorial sovereignty if their permission has not

Example on how chatbots can be used for prevention & investigation

In 2013, the Dutch children's rights organisation Terre des Hommes launched the Sweetie project. Sweetie is a virtual ten-year-old Filipino girl (i.e., an avatar) with a very lifelike appearance, which is used to identify and expose offenders in chatrooms and online forums. The Sweetie avatar was initially operated by an agent of the organisation, whose goal was to gather information on individuals who contacted Sweetie and solicited webcam sex from her. To avoid incitement, the operators would wait for individuals to initiate a conversation with Sweetie in a sexually suggestive way. Researchers were able to identify the individuals communicating with Sweetie, using only the information voluntarily provided to the avatar and by gathering publicly available information on the internet, such as Facebook or Yahoo accounts (Guyt, 2019). The gathered information was subsequently handed over to the authorities, who could then launch investigations in their respective country. To significantly expand the possibility to interact with offenders, Sweetie has been further developed into a semi-automated and, most recently, fully automated chatbot called Sweetie 3.0.

been sought in advance.

A potential way forward is the use of large language models (LLMs) to power such initiatives. For example, ChildSafe.ai amplifies the ability to identify and respond to online sexual exploitation by mobilizing chatbots. When comprehending the conversations of a potential sex buyer, ChildSafe.ai delivers a customized deterrence message in which it warns the buyer of the legal and social ramifications of buying sexual access to others (Van der Watt, 2023).

5.7 Hacking

Another method, which can be employed in digital investigations is hacking. This enables law enforcement agencies to covertly and remotely gain access to a computer/mobile device used by a suspect. Once access is gained LEAs can intercept and read out communications before encryption is activated or after it has been reversed (e.g., by using keyloggers to acquire login names, passwords, URLs and the content of messages; activating microphone and/or camera to record audio & video; activating GPS functionality to locate the device). Though effective, the use of this investigative method requires very strong legal safeguards due to the significant invasion of privacy.

5.8 Digital forensics

While there are no universally accepted subdomains in digital forensics, many experts, nevertheless distinguish between six specialised areas, divided based on the unique source of evidential information employed. These are:

1. Computer forensics

Computer forensics investigators employ an arsenal of techniques to extract and analyse evidence.

These techniques include:

- ❖ Data acquisition
- ❖ File system analysis
- ❖ Operating system analysis
- ❖ Stenography and data hiding detection.

2. Cloud forensics

Cloud forensic investigations focus on cloud-based data and infrastructure, uncovering evidence and reconstructing activities within the digital cloud.

3. Network forensics

Network forensic investigation focuses on the analysis of network traffic, logs, and infrastructure. They do not deal directly with physical devices but rather the dynamic flow of data across networks. Among the key challenges of network forensic investigations there are:

- ❖ Volatility
- ❖ Large data volumes
- ❖ Encrypted traffic.

4. Database forensics

Database forensics investigations involve the analysis of databases, including the raw data and the metadata that describe the data. There are certain unique challenges to database forensics investigations, such as:

- ❖ The diversity of data types which requires the use of specialised techniques tailored to each database format, whether relational or NoSQL.
- ❖ Difficulty in navigating the complexity of database schemas and identifying data relationships.
- ❖ Managing the volatility of transaction logs and audit logs.

5. Mobile forensics

Mobile devices are not standard and the ability of digital forensic services to access data varies between manufacturers, models, operating systems and even versions of the same model of a device and may also change over time.

It is not possible to obtain and examine every artefact or item of digital evidence from a device for analysis in every situation – there are constraints to the extent and depth of an examination in the circumstances of each case. It is critical that the investigator and prosecutor are aware of the opportunities presented by a device and the limitations and boundaries of an examination; including the implications of utilising one examination methodology over another if further work is required in the future.

While capabilities differ greatly between organisation and states, there are 3 main levels of data extraction and examination of mobile devices offered by the digital forensic services:

1. **Level 1** - a “logical” extraction. A “logical” extraction provides the live data that is readily available on device (all of the data you could see if you were able to turn on the device and browse through it). A logical extraction will extract the live data that is supported by the extraction software being used. It may not extract all of the data present and will not usually extract deleted material.
2. **Level 2** - can be either a “logical” extraction using selected tools in a laboratory environment to report that data or a “physical” extraction, capturing data that may be unallocated to a file or is associated with deleted data on a device. “Physical” downloads can extract deleted data, although again capabilities vary depending on the nature of the device, operating system, types of applications and whether they are supported by the extraction software.

3. **Level 3** - examinations are usually expert and bespoke methods to tackle complex issues or damaged devices (Code for Crown Prosecutors, 2022).

6. Social media forensics

Social media forensic investigation includes multiple categories of data, such as;

- ❖ Textual content: Posts, comments, messages, and other text-based interactions provide insights into user behaviour, opinions, and potential criminal activities.
- ❖ Multimedia evidence: Images, videos, and even audio recordings, which can provide information on location, types of criminal activities carried out and individuals involved.
- ❖ Network connections: Analysing user connections, groups, and interactions can shed light on criminal networks, organised groups, or hidden associations.
- ❖ Metadata: Timestamps, location data, and other embedded information within social media content can provide valuable context and forensic clues (Bokolo et al, 2024).

5.9 Extracting digital evidence

When it comes to digital investigations, evidence can be collected in multiple ways:

- a. **Stage 1** - OSINT investigations: this can be helpful to locate posts and their content, depending on the security settings of the account(s) being monitored

In the case of OSINT investigations, many authorities recommend keeping a record of the searches. This can be done by using body-worn cameras or by taking screenshots of what has been searched and reviewed. This being said, screenshots should be an approach of last resort when other methods have been explored or are inappropriate.

- b. **Stage 2** – Physical examination of device: This can be done either via a download using one of the methods detailed above in Section 5.8 or through manually searching/scrolling through the phone. A manual search and a 'level 1' (logical extraction) download are unlikely to reveal deleted material. Both types of physical examination will depend on the ability of the investigator to access the phone, such as knowing the PIN or pattern lock for the device.
- c. **Stage 3** – When LEAs do not have access to the devices, content information can be obtained directly from the electronic services providers (either through the voluntary provision of information or by using existing legal instruments such as the mutual legal assistance) (Code for Crown Prosecutors, 2022).

In the latter case, LEAs can collect not only subscriber information and traffic but also content data, such as stored documents, content of online conversations.

Different types of communications can be gathered:

- ❖ **Subscriber data:** this includes (a) the subscriber's identity, postal or physical address, telephone and other access number, billing and payment information, available based on the service agreement or arrangement, (b) the type of communication service used, the technical provisions taken thereto and the period of service and (c) installation of communication equipment.
- ❖ **Traffic data** (also called metadata) - can reveal the following information about a communication: its origin, destination, route, time, date, size, duration, and type of underlying service. Traffic data therefore enables law enforcement officers to learn about (a) the devices used by a suspect, (b) the internet services that a suspect is using at a specific time, and (c) the location data of a suspect's device.

- ❖ **Content data**, which can be defined as “*data with regard to the meaning or message conveyed by the communication, other than traffic data*”. This includes private messages that can be sent using electronic communication (Oerlemans, 2017).

Each of these categories, depending on the sensitivity of the data exchanges requires different safeguards.

5.10 Recovering deleted data

When it comes to digital evidence in cases of child trafficking it is important to remember that often traffickers ensure any digital exchange between them and the victim is done on encrypted platforms where messages get deleted after a time.

Telegram

Telegram's structure is complex and very challenging for forensic investigations, especially when it comes to deleted data. The first and most important distinction is whether the deleted messages are part of a normal conversation or a ‘secret chat’. Its database's characteristics (i.e., WAL journaling mode without Auto Vacuum and Secure Delete features), makes it possible to retrieve a large number of deleted records from the WAL as long as the examiner has the least interaction with the application. The consensus so far is that it is impossible to recover deleted records from the database's freelist pages. As for deleted media files (pictures) the recovery of relevant artefacts depends solely on the type of chat (normal/secret) (Vasilaras et al, 2023).

General recommendations on data recovery

Different types of tools should be tried *as they have various levels of success*. E.g., *Oxygen Forensics 14.1 could properly decode the undeleted secret media messages but not the normal ones while UFED PA 7.50 was successfully for normal ones but not the secret ones*.

It is important to use the latest versions of tools (e.g., *AXIOM 6.0 is successful where AXIOM 5.7 is not*).

Due to lack of information from application's cloud Servers, the only way to retrieve deleted messages and media files is by examining the device where the application is installed.

There are however cases where the only way to retrieve the data is by reaching out to the platforms themselves. Most platforms have dedicated law enforcement guidelines and access points, such as:

- ❖ Discord - <https://discord.com/safety/360044157931-working-with-law-enforcement>
- ❖ Snapchat - <https://values.snap.com/safety/safety-enforcement>
- ❖ Airbnb - <https://www.airbnb.co.in/help/article/960#emergency-requests>⁴
- ❖ Meta
- ❖ (Facebook/Instagram/WhatsApp) - <https://www.facebook.com/help/494561080557017>

5.11 Promising practices identified in improving public-private exchange of information in digital investigations

There are a number of promising practices identified, such as:

⁴ It is important to note that Airbnb's law enforcement portal has been extended to handle inquiries in several other languages beyond English, such as French, Spanish, German, Italian, Portuguese, Portuguese (Brazil), Korean and Japanese

1. Law enforcement authorities sharing more in-depth sensitive information and intelligence about what they are seeing and forecasting; This would include authorities providing more open access to intelligence and ongoing operations.
2. Granting higher vetting status to view such material to representatives of tech companies.
3. Ensuring that all requests for information are very clear and include all the necessary supporting legal documents, including information on operational context.
4. All law enforcement urgent requests should be in accordance with the “emergency” definition provided by the tech platforms.
5. Tech companies and tech developers should be more open and upfront about new and emerging technologies and the potential security threats of their use by criminals
6. More training provided to the trust and safety teams of companies on how to interact and cooperate with law enforcement.
7. The development of an experience exchange programme affording the opportunity for identified personnel within law enforcement agencies and tech companies to be embedded within each other’s operational functions.
8. Create permanent liaison positions, e.g., embed (or second) law enforcement personnel (e.g., data scientists) to tech companies.
9. The development of joint strategic research requirements, identifying and prioritising areas of mutual concern for further development and investigation through research (Macdonald et al, 2023).

5.12 Use of AI in digital investigations

There are various AI applications which can be successfully used in digital investigations. This is due to AI's ability to independently process large amounts of information rapidly and identify crime-related patterns.

Linguistic analysis

a. Linguistic manifestations of asymmetric power in commercial sexual exploitation

As victims must comply with the micro regulation and surveillance of perpetrators they often engage in discursive over-elaboration. The over-elaboration consists of providing details of their location, activity and timing, being designed to justify those as work and profit relevant. This pattern of pre-emptive unsolicited over-elaboration was only present in conversations with perpetrators and was almost non-existent in personal conversations with other individuals (Pomerantz et al, 2021).

b. Native language identification

Native language identification can be done using multiple techniques: (a) NLID (native language influence detection) – by seeking to indicate an author's native language, also termed L1, from the way they write in a second language (or L2); NLI (native language identification) - closely related field to NLID, seeking to indicate an author's native language, but from a computational perspective (Perkins, 2018).

c. Authorship analysis

Authorship analysis seeks to gain information on the author's linguistic and social background.

d. Identifying predatory conversations

Predatory conversation data has different characteristics when compared to non-predatory conversation data. The characteristic differences stem from the writing style between two specific persons, between classes of persons (e.g., adults versus children), or between the themes of the conversation or text.

One area of analyses are the **chat-based features**, such as:

- ❖ Ratio of initiating the topics of conversation by the user;
- ❖ The percentage of written lines by a user; and
- ❖ Time spent online.

In this context, conversation topics are mostly initiated by online perpetrators as a way to gain enough information about the victim and assess the risk. The way to achieve this is by asking many questions. When it comes to content, evidence indicates that online predators are emotionally unstable and prone to lose their temper and be anxious. In terms of chat-based features this can be identified by the types of conversations they initiate (e.g., negative, anxious).

Time when conversations take place is a further indicator. For example, chats happening late at night can be used, in combination with the other indicators, to identify predatory interactions.

e. Affective features and Linguistic Inquiry and Word Count

Linguistic Inquiry and Word Count (LIWC) provides psycholinguistic profiles for the conversations revealing the emotional and psychological aspects of the data. This can be useful when analysing cases of child offenders, as they may display feigned emotions and affection to leave the impression they are in love with the minor victim. LIWC enables the analysis of textual documents and the provision of various personal interest categories, such as love, emotion, leisure; as well as psychological categories and punctuation groups (Borj et al, 2023).

Image analysis

f. Facial recognition

This is a tool employed by investigators to identify faces by matching online images with existing records. It is employed for both victim and perpetrator identification. When facial recognition attempts to identify a face, it looks for characteristics for a match, such as jawline length, the shape of the cheekbones, and eye sockets' depth (DashMagazine, 2019).

Image analysis can also be employed for automated child nudity detection, and age estimation (Sanchez et al, 2019).

g. Empty room identification

One strategy that can be employed for identifying online content linked to trafficked images and cases of exploitation is the photographing of empty rooms of offenders. The physical characteristics of known rooms can then be linked through the use of image recognition to online content, in cases whether offenders used the same physical space to conduct/record their activities. This can be useful especially in the case of unresolved cases.

h. Age identification

The age of a subject can be judged by the face, signs of puberty, physical development, skin firmness, jawline, foreheads, cheekbones, neck, facial hair, etc. Each one of these components could constitute part of an ensemble of models to predict age by averaging the results. Nevertheless, not all of these components would be available at a given time.

The accuracy of such models is heavily dependent on the amount and quality of training input provided. Certain age groups have less amount of data, particularly the underage age range. This is a result of restrictions and ethical implications associated with setting-up datasets for this age range. In addition to increased image density in the lower age ranges, there is also a need for more gender and racial diverse datasets. Since every face is different and reflects variations in, inter alia, race, ethnicity,

gender, age and geography, neural networks can be biased in favour of external characteristics (Grübl et al, 2022).

Though there are several age labelled datasets available, these are only a start. To enrich the dataset, one must identify other sources (e.g. online sources), albeit there are a number of legal and technical restrictions in these cases as well.

There are also a number of factors which may affect systems ability to accurately determine age:

- ❖ Intrinsic components, such as size of the bone, genetics or facial changes due to the development of a child;
- ❖ Extrinsic components, such as facial expressions, noise, makeup and gender.

Facial expressions - smiling, frowning, surprise and laughing may introduce facial lines that are confused for wrinkles and thus impact on the age estimation performance.

Noise - Estimation made by impact by image brightness, colour or digital encoding during image capture and digital sharing.

Use of makeup – it can significantly influence perceived facial age estimation.

Gender – Research has shown a higher rate of error for female subjects than for males (Scanlon, 2021).

i. Nudity detection

The nudity detector is initially used to flag and filter images and be further used in conjunction with an ensemble of models that endeavour to solve a bigger problem which is the detection of illicit material related to minors. In more advanced uses of nudity detectors, different types of nudity are employed such as: normal (class 1); swimming suit (class 2); topless (class 3); nude (class 4) and sexual activity (class 5).

Integrated systems

There are multiple systems which provide integrated services aimed at assisting digital investigations into THB. One such example is the REVERSE system. When pin-locked devices are brought into the forensics team and devices are password-protected, the team tries to get around the security measures by hacking into the devices so that the content can be evaluated. The REVERSE software aims to address this gap: it also takes physical evidence collected by police officers in the field, including among other evidence types, letters, invoices, and anything else that police officers can consider as important. It then combines them with other pieces of information collected electronically and generates a list of passwords from such bits of intelligence to gain access to the device(s). If this stage fails and access to the devices is not secured by the forensics team then other legal and technical options can be considered. Table 4 introduces the links between the modus operandi of traffickers, the actions of law enforcement and the technologies that facilitate both.

Action	Technology	Actors involved	Objective	Constraining activities	Outcomes	Technology contributing to prevention/countering
Initiating online communication via proxy identities.	Social media platforms and web applications	Perpetrators – ability to connect with children by masking their real identity (e.g., photo/video manipulation)	Finding potential victims online and initiating communication	No constraints	Recruit minors	Platform age restriction/age verification mechanisms
		Law enforcement officers – masking their identities and reverse-engineer behaviour of perpetrators	Impersonate children online and communicate with perpetrators	Legal & resource constraints	Identify perpetrator with the goal of prosecution	Cognitive Chatbots; Advanced HoneyPot Techniques
Building trust	Social networks, image-editing software, face-swap apps, AI-deepfakes	Perpetrators use social media/gaming platforms to gain trust of victims often by sharing images of a sexual nature first They use video/photo manipulation software to hide their identities/appear younger	Generate realistic looking personas and imagery which they share via online platforms/apps	Real-time nude detection across some platforms/apps may prevent direct dissemination Technical restrictions in sharing multimedia with accounts held by minors	Victims start trusting perpetrator due to the exchange and more likely to respond to their requests	Trust management systems, hardware/software-based image detection
Engage in online blackmail and collection of sexual content	Hardware and cloud-based storage solutions, social media platforms & apps	Once the victim has provided multimedia content of a sexual nature to the perpetrator, the latter uses a combination of threats and extortion to keep the victim under control and further exploit them.	Receive and store child pornography online Build control over the victim with the purpose of trafficking them (online or in real-life)	Real-time nude detection in multimedia content online	Children feel forced to comply with the requests of the perpetrator and further multimedia content is produced & exchanged	Linguistic analysis Digital forensics
Traffic child imagery, encryption and monetization of imagery	P2P networks, dark web, paedophile forums, cryptocurrency	Perpetrators communicate with other perpetrators to initiate online trafficking of minors and monetization/exchange of imagery	Enhance multimedia collection by participating in trafficking networks, monetize, exchange activities	Network based detection on 2 nd generation imagery; group infiltration	Multimedia gets widely distributed in exchange for currency (e.g., cryptocurrency) or virtual tokens	P2P Network monitoring Digital forensic Cyber money laundering

					(paedopoints on dark web markets)	
Combine intelligence from multiple sources to identify perpetrators	Crime investigation software (e.g., in the UK – HOLMES 2); Intelligence systems (e.g., systems aimed at collecting and integrating intelligence)	Law enforcement units Awareness of gaps in the intelligence flow	Build perpetrator profiles from multiple sources (e.g., OSINT, HUMINT)	Data validation problems; Difficulties in integrating intelligences from multiple sources	Information exchange challenges can make it difficult to build robust profiles of perpetrators	Information exchange at different levels: technical, legal, policy
Conduct time-sensitive scans on imagery	Image analysis systems	Prioritising high risk cases and sending them for further processing	Collect enough imagery to secure prosecution	Backlog of triage analysis Outsourcing with its financial implications	Children who are victims of trafficking might be missed due to algorithmic /profile-related restrictions Volume of data requires triage otherwise there is a risk of block	Risk based approaches to online child trafficking; behavioural profiling
Posting children's photo online	Social network accounts of parents Social media accounts of schools & other entities carrying out activities with and for children Children's social media/gaming accounts	Parents share imagery of children with friends and family Entities working with children may also share their imagery to promote their activities Children share their own imagery	This imagery can be -reshared and can be employed for exploitation & it can be used for image manipulation	User appropriate warnings based on image recognition could be useful to raise awareness of risks	Child imagery is captured, distributed,	
Monitor online conversations for online indicators	Sock-puppet accounts; data crawlers	OSINT using online indicators for child trafficking	Engage in real-time interactions with potential perpetrators	False positives Complex investigations and resource intensive	Identify perpetrators Build more robust online indicators	Natural language processing; multimedia analysis; speech analysis;

		Using honeypots applying both hunting and fishing strategies	Monitoring interactions taking place on different platforms	especially maintaining honeypots active		Large-scale social media monitoring
Bypass encryption	Tools such as REVERSE	Digital forensic analysts will use hardware and software to decrypt confiscated devices	Bypass encryption by reverse social engineering and/or brute force attacks	Constrained by what can be achieved by	If access is not secured then other options can be used such as hacking (however these are significantly more problematic)	Digital forensics, Cloud forensics, Human rights safeguards
Accessing social media accounts bypassing age restrictions	Social media platforms, applications	Children gain access to these networks at a very young age	Bypass age restrictions & initiate relations with strangers; can receive money	Constraints occur when technology prevents age restrictions from being by-passed & when there is parental control	The ability of children to by-pass age restriction tools allows them to connect online but they don't realize	Cyber-security awareness Online identity management

6 Use of digital evidence in prosecution & judicial response

6.1 Challenges to investigation and prosecution

There are a number of challenges which make it even harder for cases of child trafficking to reach prosecution stage.

- a. **Over-reliance on victims' testimony.** Research has shown that to secure a charge or conviction, law enforcement officials must rely heavily on the cooperation of victim-survivors (Gallagher & Holmes, 2008; RCMP, 2010; Ward & Fouladvand, 2018).

This is particularly problematic due to a combination of factors:

- ❖ First and foremost, **many victims do not want to cooperate with the police due to fear⁵**, trauma and potential 'romantic feelings' towards their trafficker.

As a result of these, the victims display unquestioned obedience towards their abusers. They may also feel shame and fear about sharing their experience with law enforcement, especially when their credibility is being questioned, they are asked questions about their sexual history and/or when they have been asked to participate in committing criminal acts themselves (Farrell et al., 2014; Ibrahim, 2018).

- ❖ **Victims do not consider themselves victims.** Often labelled as 'Stockholm Syndrome' there are instances where victims "develop positive feelings towards their abuser and negative feelings towards the authorities [seeking] to rescue them" (RCMP, 2010, p. 39).

⁵ Fear may be in relation to their own well-being or that of their friends and/or family (Baird & Connolly, 2021; Kennedy et al., 2007; Marcus et al., 2014; Ward & Fouladvand, 2018).

This happens particularly in cases where traffickers pretend to have romantic feelings toward the victim (Ward & Fouladvand, 2018).

In such cases, victims become unable to identify their experience as victimisation and they are therefore unable and/or unwilling to cooperate with authorities.

- ❖ Initial cooperation does not mean long term cooperation. Due to the length of trafficking cases⁶ victims can change their mind about cooperation. There are multiple reasons for this, from fear of judgement or of potentially being confronted with their perpetrator or simply from a desire to rebuild their lives and leave their trauma behind.

- b. **Digital evidence required to corroborate the testimony of victims.** Law enforcement seek to collect digital evidence not so much to identify victims, but to corroborate their stories and identify potential witnesses.

The reason for this is the high unreliability of victims' testimonies. This is due on one hand to trauma and on the other to intentional efforts made by traffickers to confuse their victims (e.g., through frequent location changes, forced drug consumption) (Ballucci et al, 2022).

⁶ In some cases, these can span over many years.

6.2 Interpretation of emojis in court proceedings

Emojis can become key pieces of evidence in cases of child trafficking. This is because an emoji can change the entire meaning of the subsequent words or sentences, especially as in many THB-related content emojis replace full words and phrases (see People Vs. Jmerson case, Parise, 2020). Considering this, it is important for courts experts to be appointed who can provide adequate interpretation of emojis and their use in criminal contexts.

Example of emoji use in a human trafficking case

In the case People v. Jamerson, involving a human trafficking operation the court analysed emojis from text messages to determine whether this was indeed a case of trafficking. An important piece of evidence was a crown emoji used in a text message exchange between a trafficker and their victim. Testimony from an expert in the area of sex trafficking was needed to help in the interpretation of the crown emoji. While the emoji could have been in multiple ways, the expert witness opined that a crown is an emoji “specific to commercial . . . sexual exploitation.” The expert interpreted the crown emoji to signify “the pimp is king.”

7 Legal framework related to the collection, analysis and preservation of digital evidence

This section focusses on the legal framework changes needed for the effective collection, analysis, and preservation of digital evidence in human trafficking cases. It identifies current gaps and recommend updates to enhance the use of digital evidence.

Digital evidence is any electronic data or information that can be utilised as evidence in a legal investigation or court case. This evidence can be gathered through a range of methods, including forensic imaging of seized devices, data recovery from storage media, capturing network traffic, and extracting metadata from files (Caseu, 2011).

When compared to traditional evidence, **digital evidence presents unique authentication challenges due to the sheer volume of data available, its rapid creation and transfer, its susceptibility to quick deletion or overwriting and its vulnerability to manipulation, alteration, or damage.** Some countries have established rules of evidence with authentication criteria tailored to digital evidence, while others apply similar authentication standards to both traditional and digital evidence.

In that respect legal standards are essential for the collection of digital evidence, as they help maintain its integrity, reliability, and admissibility in court. These standards provide guidelines for the processes involved in collecting, handling, storing, and presenting digital evidence to prevent tampering, contamination, or data loss.

To ensure evidence is admissible, it must be gathered in compliance with procedural rights and relevant laws. Failure to meet these legal requirements may result in the exclusion of digital evidence from legal proceedings, potentially affecting the case's outcome.

The collection of digital evidence involves capturing data from social media, online databases, and public records, which can later become pivotal in building a case. While this type of collection does not always follow the stringent procedures of formal digital evidence collection, it requires a keen understanding of digital landscapes and the legal implications of using such information. In that respect here are some examples of digital evidence commonly collected in human-trafficking cases such as (Latonero, 2011):

- ❖ **Social Media Accounts:** Posts, messages, and interactions on platforms like Facebook, Instagram, Twitter, and Snapchat can provide insights into trafficking networks and victim interactions.
- ❖ **Text Messages:** SMS and messaging app conversations (e.g., WhatsApp, Telegram) can reveal communication patterns between traffickers and victims.
- ❖ **Emails:** Correspondence that may contain agreements, arrangements, or discussions related to trafficking activities.
- ❖ **Website and Chat Logs:** Data from websites or chat rooms used for recruiting, advertising, or facilitating trafficking, including postings on online classifieds and escort services.
- ❖ **GPS Data:** Location information from mobile devices can help track the movements of victims and traffickers.
- ❖ **Photos and Videos:** Multimedia files found on devices or social media that can document the conditions and treatment of victims, as well as connections to traffickers.
- ❖ **Payment Records:** Transaction logs from digital payment services, revealing financial exchanges related to trafficking activities.

- ❖ **Surveillance Footage:** Video recordings from public or private cameras that capture the movements of individuals suspected of being involved in trafficking.
- ❖ **Search History:** Browsing data from computers or mobile devices that may show searches related to human trafficking, prostitution, or other illicit activities.
- ❖ **Mobile Applications:** Specific apps that may be used for communication, advertising, or facilitating trafficking operations.

Different forms of digital evidence require specialised methods and tools for their collection, preservation, and analysis, underscoring the necessity of technical expertise in digital forensics. Upholding the integrity and authenticity of this evidence is vital to ensure its admissibility in legal proceedings.

In respect to preservation of digital evidence in human trafficking cases in the EU, law enforcement agencies must adhere to the principles of legality, necessity, and proportionality. This includes obtaining proper authorization for data collection, ensuring the integrity of the evidence through chain of custody procedures, and respecting the rights of victims and suspects. Preserving digital evidence is important, especially when it is related to human trafficking cases and has the potential to further the investigative process. Many different methods are used to preserve digital evidence.

These methods for preserving digital evidence to ensure its integrity and admissibility in legal proceedings include (Granja et al, 2017):

- ❖ **Generating forensic images** involves creating an exact duplicate of the digital evidence, referred to as a forensic image, to maintain the integrity of the original data. This copy allows for analysis without modifying the primary evidence.
- ❖ **Keeping thorough documentation of the chain of custody** is essential for verifying the integrity of the evidence by recording all individuals who accessed the evidence, the timing of access, and the reasons for access.

- ❖ **Creating cryptographic** hash values of digital evidence through hashing can assist in verifying its integrity by confirming that the data has not been altered during the preservation process.
- ❖ **Employing write-blocking technology**, either hardware or software, prevents any modifications to the original evidence while preserving it, thereby safeguarding its integrity.
- ❖ **Storing digital evidence in a secure and controlled environment**, such as an encrypted storage device, helps prevent unauthorised access or tampering.

Keeping detailed documentation of the preservation process, including the methods used, dates and times of actions taken, and individuals involved, is essential for establishing the authenticity and reliability of the evidence. By following these methods for preserving digital evidence, investigators can ensure that the integrity of the evidence is maintained and that it can be effectively used in legal proceedings.

To effectively collect, analyse, and preserve digital evidence in human trafficking cases, several legal framework changes have to be implemented. These changes could include:

- ❖ **Clarifying laws regarding the admissibility of digital evidence in court**, ensuring that such evidence is treated with the same level of credibility as physical evidence. This involves establishing clear guidelines and standards for the collection, preservation, and presentation of digital evidence in legal proceedings.
- ❖ **Implementing stricter regulations on data retention by internet service providers and social media platforms** to ensure that crucial evidence is not lost or deleted in human trafficking cases. By requiring these entities to retain data for a specified period of time, law enforcement agencies can have access to valuable information that may be critical in investigations and prosecutions. These regulations could include mandates for the retention of user activity logs, communication records, and other relevant data that could potentially serve as evidence in

human trafficking cases. Additionally, guidelines for the secure storage and preservation of this data should be established to prevent tampering or unauthorised access.

- ❖ **Enforcing stricter data retention regulations**, authorities can enhance their ability to collect and analyse digital evidence, ultimately strengthening their efforts to combat human trafficking and bring perpetrators to justice. By working together, these stakeholders can leverage their respective expertise, resources, and best practices to enhance investigative efforts and support prosecution outcomes. In this respect law enforcement agencies play a key role in investigating human trafficking cases and collecting digital evidence.
- ❖ **Collaboration between technology companies, law enforcement agencies and NGOs through accessing specialised tools and expertise for extracting and analysing digital data from various devices and platforms**. Technology companies can also provide valuable insights into emerging technologies and trends that may impact digital evidence collection. Non-governmental organisations (NGOs) often have on-the-ground experience working with victims of human trafficking and can provide valuable support in identifying and preserving digital evidence. They can also offer training and resources to law enforcement agencies on best practices for victim-centred investigations and evidence collection. Collaboration between these stakeholders can help establish standardised protocols for digital evidence collection and analysis, ensuring that evidence is handled in a consistent and legally sound manner. By sharing knowledge and resources, law enforcement agencies, technology companies, and NGOs can collectively work towards combating human trafficking more effectively and bringing perpetrators to justice.

In this regard, it's crucial to equip law enforcement agencies with the appropriate resources and training needed to efficiently collect and analyse digital evidence. This includes the utilisation of specialised forensic tools designed for in-depth examination and interpretation of digital data. To

enhance the effectiveness of these experts in human trafficking cases, the following guidelines have to be considered:

- ❖ **Qualification standards:** Establish clear criteria for the qualifications and expertise required of digital forensic experts, including relevant education, training, certifications, and experience in the field of digital forensics.
- ❖ **Continuous education:** Encourage digital forensic experts to keep with evolving technologies and methodologies through ongoing training and professional development opportunities.
- ❖ **Admissibility standards:** Define the criteria for the admissibility of digital evidence and the testimony of digital forensic experts in court, ensuring that their methods and findings meet the necessary legal standards.
- ❖ **Testimony guidelines:** Provide guidelines for digital forensic experts on how to effectively communicate their findings in court, including the use of clear and concise language, visual aids, and expert reports to support their testimony.
- ❖ **Cross-examination preparation:** Prepare digital forensic experts for cross-examination by opposing counsel, ensuring they are able to defend their methods, findings, and conclusions under scrutiny.

By implementing these guidelines for the qualification and testimony of digital forensic experts, authorities can strengthen the credibility and reliability of digital evidence in human trafficking cases, ultimately improving the chances of successful prosecution and justice for victims.

Another important point that has to be considered is strengthening international cooperation and information sharing mechanisms to facilitate the cross-border investigation of human trafficking cases involving digital evidence. This can be achieved through several key strategies (UNODC, 2020):

- ❖ **Establishing formal agreements and protocols** between countries to streamline the exchange of digital evidence in human trafficking cases. This could involve mutual legal assistance treaties, extradition agreements, and information-sharing frameworks.
- ❖ **Enhancing communication channels** between law enforcement agencies across borders to facilitate real-time collaboration and coordination in investigations. This could include the establishment of dedicated task forces or joint investigation teams focused on combating human trafficking.
- ❖ **Promoting the standardisation of digital evidence collection and analysis practices** internationally to ensure consistency and compatibility between different jurisdictions. This could involve the development of common protocols, training programs, and certification standards for digital forensic experts.
- ❖ **Leveraging international organisations and platforms**, such as INTERPOL and Europol, to facilitate the exchange of intelligence, best practices, and resources in combating human trafficking. These organisations can serve as valuable hubs for information sharing and coordination among member states.

By strengthening international cooperation and information sharing mechanisms, authorities can overcome the challenges posed by cross-border investigations in human trafficking cases involving digital evidence. This collaborative approach is essential for effectively combating this global crime and holding perpetrators accountable across jurisdictions.

In addition to the previously mentioned legal framework changes, further measures may be necessary to enhance the collection, analysis, and preservation of digital evidence in human trafficking cases. Such as:

- ❖ **Standardising protocols** for the handling and storage of digital evidence to ensure its integrity and admissibility in court. This could involve establishing guidelines for the chain of custody, data encryption, and secure storage practices.
- ❖ **Implementing data privacy regulations** that balance the need for law enforcement access to digital evidence with the protection of individuals' privacy rights. This could involve developing clear guidelines on when and how digital evidence can be obtained and used in investigations.
- ❖ **Enhancing collaboration** between law enforcement agencies, technology companies, and non-governmental organisations to facilitate the sharing of expertise, resources, and best practices in digital evidence collection and analysis.
- ❖ **Investing in research and development** of advanced technologies for digital forensics, such as artificial intelligence and machine learning algorithms, to improve the efficiency and accuracy of evidence analysis.

By addressing these additional considerations and implementing comprehensive legal framework changes, authorities can better equip themselves to effectively combat human trafficking through the collection, analysis, and preservation of digital evidence.

Another very important instrument regarding human trafficking cases in the context of electronic evidence is the SIRIUS system related to Eurojust. The SIRIUS system is a secure communication and information exchange platform used by Eurojust, the European Union's agency for judicial cooperation in criminal matters.

This system allows national authorities, such as prosecutors and law enforcement agencies, from EU Member States to securely share information, coordinate investigations, and collaborate on cross-border criminal cases. SIRIUS facilitates the exchange of sensitive data, such as evidence, intelligence, and legal documents, while ensuring compliance with data protection regulations and confidentiality requirements.

The system enhances communication and coordination among EU Member States, helping to overcome legal and procedural obstacles that may arise in cross-border investigations and prosecutions.

In that sense another important tool that should be mentioned is the SIENA System related to EUROPOL. The SIENA system is a secure communication platform used by EUROPOL, the European Union Agency for Law Enforcement Cooperation. This system allows for the exchange of sensitive information and intelligence between EUROPOL and its law enforcement partners across Europe. The SIENA system plays a crucial role in facilitating collaboration and coordination in the fight against transnational crime, including human trafficking, terrorism, and cybercrime.

Through the SIENA system, authorised users can securely share operational data, analytical reports, and strategic assessments to support joint investigations and operations. The system is designed to ensure the confidentiality, integrity, and availability of information shared among EUROPOL member states, enabling swift and effective responses to emerging threats and criminal activities.

Some final important instruments are the European Production Order and the European Preservation Order (EU Regulation 2023/1543) and the so-called Joint Investigation Teams (JIT).

European Production Orders (EPOs) are a legal instrument established by the European Union to facilitate the cross-border gathering of electronic evidence in criminal investigations. EPOs allow judicial authorities in one EU member state to request electronic evidence directly from service providers located in another member state, without the need for mutual legal assistance treaties (Article 3(1) EU Regulation 2023/1543).

EPOs streamline the process of obtaining digital evidence by providing a standardised and expedited procedure for requesting and obtaining data, such as emails, documents, and other digital information, for use in criminal proceedings. This mechanism aims to improve the efficiency and effectiveness of

investigations by reducing bureaucratic hurdles and delays associated with traditional mutual legal assistance procedures (Article 3(1) EU Regulation 2023/1543).

The implementation of EPOs is part of the EU's broader efforts to enhance judicial cooperation in criminal matters and combat cross-border crime, including human trafficking. By enabling law enforcement authorities to swiftly access electronic evidence across EU borders, EPOs contribute to the effective collection, analysis, and preservation of digital evidence in criminal cases, including those related to human trafficking.

The European Preservation Order for electronic evidence is a legal instrument that allows for the preservation of electronic evidence in civil and commercial matters across EU member states. This mechanism enables parties to secure and protect electronic data that may be relevant to a particular case, ensuring its integrity and availability for future proceedings. The European Preservation Order for electronic evidence aims to facilitate the collection and preservation of digital information in a cross-border context, enhancing the efficiency and effectiveness of legal proceedings involving electronic data (Article 3(2) EU Regulation 2023/1543).

A Joint Investigation Team (JIT) is a collaborative effort among law enforcement agencies, often from different countries, to investigate complex crimes such as human trafficking, drug trafficking, cybercrime, and terrorism. When it comes to electronic evidence, a JIT can significantly enhance the effectiveness of investigations. They are set up for specific criminal investigations with a cross border impact and for a limited period of time. This framework allows the competent judicial and law enforcement authorities involved to organise and coordinate their actions jointly and investigate efficiently even in very complex cases such as trafficking in human beings (European Commission, 2021). Identifying and addressing gaps in the use of digital evidence in human trafficking cases is crucial for improving investigations and prosecutions in this complex area. Some current gaps that could be addressed to enhance the use of digital evidence in human trafficking cases include:

- ❖ **Training and Resources:** Providing law enforcement agencies, prosecutors, and forensic examiners with specialised training and resources on digital evidence collection, analysis, and preservation specific to human trafficking cases.
- ❖ **Collaboration and Information Sharing:** Enhancing collaboration and information sharing among different agencies and organisations involved in combating human trafficking to ensure that relevant digital evidence is identified and utilised effectively.
- ❖ **Technology and Tools:** Investing in advanced technology and tools for digital evidence analysis, such as artificial intelligence and machine learning algorithms, to process large volumes of data and identify patterns indicative of human trafficking activities.
- ❖ **Legal Framework:** Developing clear guidelines and protocols for the collection, handling, and admissibility of digital evidence in human trafficking cases to ensure compliance with legal standards and protect the rights of victims and defendants.
- ❖ **Victim-Centred Approach:** Adopting a victim-centred approach to digital evidence collection, taking into account the privacy and safety concerns of victims and survivors of human trafficking while gathering and using digital evidence in investigations and court proceedings.

By addressing these gaps and implementing strategies to enhance the use of digital evidence in human trafficking cases, law enforcement agencies and prosecutors can strengthen their ability to identify and prosecute perpetrators, protect victims, and prevent future instances of human trafficking. Furthermore, by encouraging continuous review, enhancement of legal instruments, and vigilance against potential abuses, legal professionals can ensure that electronic evidence is handled ethically and in accordance with procedural safeguards. Promoting collaboration, knowledge-sharing, and adherence to legal standards are essential in navigating the complexities of electronic evidence gathering in a rapidly evolving digital landscape.

In conclusion, the effective collection, analysis, and preservation of digital evidence in human trafficking cases require a comprehensive approach that encompasses legal framework changes, standardised protocols, data privacy regulations, collaborative efforts, and technological advancements. By implementing these recommendations, authorities can enhance their capabilities to combat human trafficking and ensure that perpetrators are held accountable for their crimes. It is crucial for stakeholders to work together towards a common goal of leveraging digital evidence to bring justice to victims and prevent future instances of exploitation.

7.1 Guidelines on cross-border cooperation procedures in terms of collection and exchange of digital evidence

Ensuring effective cross-border cooperation for the collection and exchange of digital evidence in child trafficking cases is extremely important, due to the international nature of the crime.

In order to enable effective and safe cooperation between Member States, the EU and the Council of Europe have established a number of legal acts and mechanisms for cross-border cooperation procedures pertaining to the gathering, storing and sharing of digital evidence. These procedures are necessary to handle the difficulties brought about by the digital character of trafficking in human beings today, which often involve data stored in different jurisdictions.

European Legal Framework for Cross-Border Cooperation

❖ Budapest Convention on Cybercrime

The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, is the most well-known legal framework for combating cybercrime in a global context. It is a binding

international treaty that aims to combat cybercrime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. The Convention covers crimes committed over the Internet and other computer networks, such as fraud, copyright infringements, child pornography, and network security breaches.

Notably, the Budapest Convention covers investigative procedures related to "the collection of evidence in electronic form" for any type of criminal offence where such electronic evidence may be relevant (Article 14 (1) and 14 (2)). It obliges Member States to adopt such legislative and other measures as may be necessary to establish the powers and procedures for the collection of such evidence. Therefore, its scope extends beyond problems of cybercrime.

A significant addition to the Convention is its Protocol on enhanced co-operation and disclosure of electronic evidence (Council of Europe, 2021). The Protocol provides tools for the obtainment and disclosure of electronic evidence in transborder cases, for instance, by allowing for direct cooperation with service providers in foreign jurisdictions, as well as the expedited disclosure of data in emergency situations where lives are at risk. Importantly, the Protocol requires that the use of these tools is carried out in an ethical manner and in accordance with the rule of law and EU human rights and values.

❖ Directive 2014/41/EU and the European Investigation Order

Traditional mutual legal assistance (MLA) procedures can be time-consuming and inefficient, often taking months to process. To remedy this, Directive 2014/41/EU aims to simplify and speed up cross-border criminal investigations in the EU by introducing the European Investigation Order (EIO), which allows for quicker access to necessary evidence and enables judicial authorities in one EU country ('the issuing state') to request that evidence be gathered in and transferred from another EU country ('the executing state'). While the text of the Directive itself does not refer to electronic evidence, its wide

scope has allowed prosecution services to efficiently use it as an instrument to obtain such evidence in international matters. To date, the European Investigation Order (EIO) has been the most effective tool for facilitating the exchange of electronic evidence across the EU. However, this will be superseded by Regulation (EU) 2023/1543, as described above, once it comes into effect.

The EIO improves on existing EU laws covering this field by setting strict deadlines for gathering the evidence requested and by limiting the grounds for refusing such requests. The executing authority must decide on the recognition or execution of the EIO within 30 days of its receipt, unless grounds for postponement exist or the evidence is already possessed by the executing State. If the executing authority cannot meet these deadlines, it must promptly inform the issuing State of the reasons for the delay and the estimated additional time needed, with a possible extension of up to 30 days. The investigative measure must be carried out without delay and within 90 days of the decision. The executing state can only refuse to act on the request under certain circumstances, e.g. if the request is against the country's fundamental principles of law or harms national security interests. All costs of acting on a request must be paid by the executing state

As the EIO is based on the mutual recognition principle, each EU country is obliged in principle to recognise and carry out such a request. It must also be done swiftly and without any further formality.

❖ Directive (EU) 2017/541 on Combating Terrorism — Impact on Fundamental Rights and Freedoms

The Directive on Combating Terrorism aims to “adapt EU law to fight terrorism”, by establishing definitions, sanctions and measures related to terroristic offences and for the protection and support of victims of such offences (Article 12 (3)).

The Directive also provides useful tools for the collection and certain forms of electronic evidence and is a useful source in cases of transborder human trafficking. Article 20(1) of the Directive requires that

investigative tools used in organised crime, or other serious crime cases, be available for authorities to investigate and prosecute terrorist and related offences. The tools listed involve searching personal property; interception of communications; covert surveillance, including electronic surveillance; audio and visual recording of persons in public or private vehicles and places; and financial investigation (recital 21). According to the Directive, such tools should respect fundamental rights and freedoms (Article 23 and recital 35), as well as EU law on the procedural rights of suspects and accused persons (recital 36) (European Union, 2017).

❖ Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings⁷

Regulation 2023/1543 addresses the need for the adoption of effective measures and mechanisms for obtaining and preserving electronic evidence in criminal investigations and prosecutions across the EU. It further emphasises the importance of implementing mechanisms that are compliant with fundamental rights and principles established under the Treaty of the European Union (TEU) and the Charter of Fundamental Rights of the European Union (the Charter). Such are, for instance, the principles of necessity and proportionality, due process, privacy and personal data protection, as well as confidentiality of communications.

The document stresses the increasing importance of electronic evidence in criminal proceedings, as well as the need for law enforcement authorities and judicial authorities to have effective tools to investigate and prosecute criminal acts related to or carried out with the help of cyberspace. It establishes the guidelines for a Member State authority to issue a European Production Order or a European Preservation Order during criminal proceedings. These orders compel a service provider,

⁷ Applicable from 17 August 2026

offering services within the Union and either established or represented by a legal entity in another Member State, to produce or preserve electronic evidence, irrespective of where the data is stored (Regulation 2023/1543).

The 2023/1543 Regulation is applicable to all service providers operating within the Union (Article 1(1)). A "service provider" refers to any natural or legal person offering one or more of the categories of services listed in the Regulation (Article 2(1)). These include electronic communications services (Article 3(3)a), which are typically provided for remuneration via electronic communications networks.

This category encompasses:

- ❖ internet access services as defined in Regulation (EU) 2015/2120,
- ❖ interpersonal communications services, and
- ❖ services primarily involving the conveyance of signals, such as transmission services used for machine-to-machine communication and broadcasting.

Additionally, service providers include those offering internet domain name and IP numbering services, such as:

- ❖ IP address assignment,
- ❖ Domain name registry,
- ❖ Domain name registration, and
- ❖ Related privacy and proxy services (Article 3(3)a).

Finally, service providers encompass other information society services as defined in Directive (EU) 2015/1535, which either enable user communication or facilitate data storage or processing on behalf of users, with data storage being a defining component of the service provided (Article 3(3)b). Furthermore, the Regulation sets out several conditions for the issuing of a European Production Order. For instance, it provides that a European Production Order to **obtain traffic or content data**

shall only be issued for the following offences, if they are wholly or partly committed by means of an information system:

- ❖ Offences concerning sexual abuse, (Article 3(3)b);
- ❖ Offences concerning sexual exploitation (Directive 2011/92/EU, Article 3);
- ❖ Offences concerning child pornography (Directive 2011/92/EU, Article 4);
- ❖ Solicitation of children for sexual purposes (Directive 2011/92/EU, Article 5);
- ❖ Incitement, aiding and abetting, and attempt of the abovementioned offence (Directive 2011/92/EU, Article 6).

Therefore, technology-facilitated child trafficking for the purpose of sexual exploitation falls within the scope of the Regulation.

Such an order should be addressed to the service provider acting as controller in accordance with the GDPR. By way of exception, the European Production Order may be addressed directly to the service provider that processes the data on behalf of the controller (see Table 5 below).

A European Production Order shall include the following information	A European Preservation Order shall include the following information
The issuing authority and, where applicable, the validating authority.	The issuing authority and, where applicable, the validating authority.
The addressee of the European Production Order as referred to in Article 7.	The addressee of the European Preservation Order as referred to in Article 7.
The user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as username, login ID or account name to determine the data that are being requested.	The user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as username, login ID or account name to determine the data for which preservation is requested.

The requested data category as defined in Article 3, points (9) to (12).	The requested data category as defined in Article 3, points (9) to (12).
If applicable, the time range of the data for which production is requested.	If applicable, the time range of the data for which preservation is requested.
The applicable provisions of the criminal law of the issuing State.	The applicable provisions of the criminal law of the issuing State.
In emergency cases as defined in Article 3, point (18), the duly justified reasons for the emergency.	The grounds for determining that the European Preservation Order fulfils the conditions of necessity and proportionality under paragraph 2 of this Article.
In cases where the European Production Order is directly addressed to the service provider that stores or otherwise processes the data on behalf of the controller, a confirmation that the conditions set out in paragraph 6 of this Article are met.	
The grounds for determining that the European Production Order fulfils the conditions of necessity and proportionality under paragraph 2 of this Article.	
A summary description of the case.	

Table 5 - Information requested for EPOC and EPOC-PR

- ❖ Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings⁸

⁸ Applicable from 17 February 2026

The aim of the Directive is to establish harmonised rules for the designation of designated establishments and the appointment of legal representatives by service providers offering services in the Union. The purpose of this is to assist in receiving, adhering to and enforcing decisions and orders issued by Member State authorities who are competent in gathering electronic evidence in criminal proceedings.

The Directive applies to decisions and orders for gathering electronic evidence based on Regulation (EU) 2023/1543, Directive 2014/41/EU, and the Convention on Mutual Assistance in Criminal Matters between Member States of the EU. It further applies to decisions and orders based on national law addressed to a natural or legal person acting as a legal representative or designated establishment of a service provider on the territory of a Member State.

In the European Union, service providers must have a defined institution that will receive decisions and orders (Directive 2011/92/EU, Article 7). For those offering services outside Europe, service providers shall result into appointing lawyers from states which they operate directly in (EU Directive 2023/1544). Service providers not established in the Union must appoint a legal representative in Member States where they offer services (EU Directive 2023/1544, Article 3(1)a).

Service providers established in Member States not participating in the relevant instruments must appoint a legal representative in Member States that do participate (EU Directive 2023/1544, Article 3(1)b).

7.2 Challenges

Some of the challenges in implementing the legislation on digital evidence include:

- ❖ The required technical knowledge for understanding the ever-changing digital technology and the data nature contributes to the frustration and inefficiency of the involved investigators
- ❖ Large volumes of data to be processed.
- ❖ The investigators must ensure that they abide by applicable laws or otherwise risk that the seized exhibits will be declared inadmissible at trial.
- ❖ Jurisdictional conflicts and disparities in legal systems.
- ❖ Cultural and language barriers.
- ❖ Ethical challenges.

7.3 Ethical Consideration in Collecting Electronic Evidence

Ethically, the collection, storage and use of electronic evidence in criminal matters, especially ones with high level of sensitivity as trafficking of children, raises various concerns. Therefore, it must be ensured that such processes respect fundamental rights, maintain the integrity of the evidence, and uphold the principles of justice.

Recommendations ensuring the ethical collection of electronic evidence in child trafficking cases are provided below.

It is important to enhance the use of digital evidence in legal investigations and court cases, related to human trafficking it should be considered implementing the following updates which will effectively protect the public and deliver justice where and when needed:

- ❖ **Legality and Jurisdiction** - A key challenge in cross-border cooperation in criminal matters, and specifically cross-border request for electronic evidence, is that each country has its own laws and regulations in terms of evidence collection and preservation. Therefore, LEAs and other relevant professionals must ensure that evidence collection follows the laws of both the country where the evidence is gathered and the country asking for it. Show respect for sovereignty and don't access data in other jurisdictions.
- ❖ **Privacy and Data Protection** – The collection of electronic evidence may violate the right to privacy of the parties involved. When collecting such evidence, professionals should do so in accordance with the Law Enforcement Directive, which sets out strict rules on how to process, collect, store, and move personal data. They must ensure that data collection methods do not violate privacy rights.
- ❖ **Consent and Notification** – Whenever feasible, the professionals collecting electronic evidence should inform the data subjects of the collection of their data, inform them about the process, the reason and the rights they have, unless that would hurt the investigation.
- ❖ **Confidentiality** - The confidentiality and sensitivity of the information related to child victims must be maintained to protect their dignity and privacy.
- ❖ **Proportionality and Minimisation** – The collection of digital evidence should be proportionate to the investigation's needs and limited to what is strictly necessary.
- ❖ **Human Rights Considerations** – Authorities must balance the need for effective law enforcement with the protection of individual rights, ensuring that all actions are transparent, accountable, and proportionate.
- ❖ **Victim-Centred Approach** - Investigators must use trauma-informed practices to minimise re-traumatisation of child victims during the evidence collection process.

- ❖ **Effective Regulations** - Law enforcement and labour inspectorates should implement stronger regulations and increased monitoring of job advertisement websites, recruiters and recruitment agencies. This could be done with the support of technological tools developed in cooperation with private companies.
- ❖ **Continuous Training** - Training on electronic evidence should be made integral to training curricula for law enforcement and labour inspectorate and be constantly kept up-to-date due to the fast-changing technological and behavioural landscape.
- ❖ Prosecutors should be provided with **specific training on technology-facilitated trafficking of human beings**, the handling of electronic evidence as well as its presentation before a judge/jury and, procedures to request electronic evidence from private companies as well as obtain evidence and cooperation from other countries.
- ❖ **Collaboration with Experts**: Collaborate with digital forensic experts and consultants to assist in complex cases and ensure the proper handling of digital evidence.
- ❖ **Continuous Improvement**: Regularly review and update digital evidence collection protocols and practices to adapt to evolving technologies and legal requirements.

8 Public-Private Partnerships in Combating Trafficking in Human Beings (THB)

8.1 General description

Public-private partnerships (PPPs) play a crucial role in combating trafficking in human beings (THB). These collaborations between governments, the private sector, and NGOs are crucial for implementing comprehensive anti-trafficking strategies. The following guidelines (cf. GRETA 2020) outline how states can leverage PPPs to enhance their anti-trafficking efforts:

Facilitating Labour Market Access

- ❖ **Economic and Social Inclusion:** States should promote the economic and social inclusion of THB victims by facilitating their access to the labour market. This can be achieved by offering vocational training, language courses, and job placement services. These initiatives not only help victims rebuild their lives but also integrate them into the broader economy.
- ❖ **Raising Employer Awareness:** Governments and NGOs should work together to raise awareness among potential employers about the benefits of hiring THB victims. This includes educating employers on how they can support victims' reintegration into society and the workforce.
- ❖ **Promoting Micro-Businesses and Social Enterprises:** Encouraging the development of micro-businesses and social enterprises can provide meaningful work opportunities for THB victims. PPPs can play a pivotal role in creating and supporting these ventures, offering victims a path to economic independence.

Support for Asylum Seekers:

- ❖ **Access to Self-Employment:** States should ensure that asylum seekers eligible for self-employment have effective access to the labour market. This includes providing vocational and language training tailored to their specific needs. By doing so, states can prevent further vulnerabilities and facilitate the economic integration of these individuals.

Strengthening Engagement with the Private Sector:

- ❖ **Corporate Responsibility:** In line with the UN Guiding Principles on Business and Human Rights and the Council of Europe Committee of Ministers Recommendation CM/Rec (2016)3, states should encourage private sector engagement in anti-trafficking efforts. Businesses have a significant role and responsibility in supporting the rehabilitation and recovery of THB victims.
- ❖ **Access to Effective Remedies:** The private sector can contribute by providing victims with access to effective remedies, such as compensation and support services. Companies should also adopt and implement policies that prevent exploitation within their supply chains and operations.

By following these guidelines, states can effectively utilize public-private partnerships to combat THB, support victims, and promote a more just and inclusive society.

8.2 Promising Practices of Public-Private Partnerships: Case Studies

Uganda: Trafficking in Persons Criminal Justice Enhancement (2019-2023):

The Human Trafficking Institute (HTI) implemented practices in Uganda to enhance prosecutions of traffickers. Key practices included embedding experts with investigators and prosecutors to foster prosecution-led investigations, which help to halt traffickers and rescue victims. Another promising practice was the introduction of plea bargaining, which mitigates the trauma of victims by avoiding the need for their testimony, reduces trial length, and increases the conviction and sentencing of traffickers. These measures have also facilitated victim restitution and compensation, thereby addressing current and future vulnerabilities.

Safe Migration in Central Asia (2019-2024):

This project, covering Kazakhstan, Kyrgyz Republic, Turkmenistan, and Uzbekistan, aimed to enhance the accountability of all stakeholders, including governments, NGOs, and the private sector, in preventing trafficking, protecting survivors, and promoting safe migration. Notable outcomes from 2020-2021 include reaching over 700,000 individuals with awareness campaigns, training more than 600 government and civil society employees, and providing humanitarian assistance and legal advice to nearly 2,000 migrants affected by the COVID-19 pandemic.

CoMensha (Coordination Center against Human Trafficking) in the Netherlands

CoMensha is the Dutch national coordination centre for human trafficking. It serves as a central hub for collecting data, coordinating care for victims, and providing information and expertise on human trafficking. Among its key activities are:

- ❖ **Victim Registration:** CoMensha manages the registration of human trafficking victims in the Netherlands, ensuring accurate data collection and analysis.
- ❖ **Referral Services:** It provides a network of shelters and support services to ensure victims receive the necessary assistance, including housing, medical care, and legal support.
- ❖ **Awareness and Training:** CoMensha conducts training and awareness programs for professionals, such as law enforcement, healthcare workers, and social service providers, to help them recognize and respond to trafficking cases.

A promising practice associated with CoMensha is its 4Ps framework—Protection, Prevention, Prosecution, and Partnership, which has been pivotal in advancing anti-trafficking efforts. The framework's 4PS stand for:

- ❖ **Protection:** Empowering survivors and establishing services to protect at-risk groups.
- ❖ **Prevention:** Working with local communities to influence social norms and reduce trafficking risks.
- ❖ **Prosecution:** Improving legal responses to trafficking cases.
- ❖ **Partnership:** Fostering collaboration among various stakeholders to strengthen policies and data collection.

Overall, public-private partnerships are instrumental in providing comprehensive responses to THB, supporting victims, and holding traffickers accountable. These partnerships enhance the capacity of all involved parties to tackle the complex issues associated with trafficking.

Applying MARAC to Human Trafficking

Multi-Agency Risk Assessment Conferences (MARACs) are collaborative meetings, originating in the UK, involving the key case workers from different organisations. Originally developed to address domestic violence, MARACs aim to ensure the safety of high-risk individuals by facilitating communication between relevant agencies, such as police, social services, victim organisations, health care, child welfare. They focus on risk assessment and developing comprehensive safety plans. Applying the MARAC model to fighting human trafficking can enhance coordination between stakeholders, improve victim support, and facilitate proactive risk management.

- ❖ **Risk Identification and Assessment** - Through MARAC's multidisciplinary approach various agencies such as police, social services, healthcare providers, NGOs, and immigration services cooperate in identifying and assessing the risk of trafficking victims. They compile the available (and sharable) data each organisation has regarding the case.

Individual and experience-based risk assessments of a case, are validated and through evidence-based risk assessment tools. MARACs use structured tools and questionnaires designed to identify the risk levels of potential trafficking victims. These tools should account for various forms of exploitation, including sexual and labour exploitation. The multidisciplinary setting confronts different professional lenses and perspective to minimise blind spots and improve shared accountability for the decisions taken.

The aim is to develop comprehensive risk profiles for identified victims, considering factors like age, gender, immigration status, and psychological state, as well as the threat and forms of violence exerted by the trafficker.

- ❖ **MARAC Meetings for Human Trafficking** - The regular MARAC meetings are dedicated to human trafficking cases. These meetings should be scheduled frequently to ensure timely

intervention and support. Meetings can be case specific (operative dimension) but also include changing trends, modus operandi, victim demography and needs (strategic dimension).

One of the key challenges of MARACs is to establish protocols for sharing sensitive information securely among MARAC participants to protect the privacy of victims and respect the various professional secrecy obligations, while enabling effective risk management.

The MARAC approach recommends action-oriented discussions, meetings on discussing specific cases, assessing risks, and developing coordinated action plans. It is crucial that each participant understands their role and responsibilities in implementing the plan. Each participant to this multi-agency conference, must have the commitment of their organisation of origin to implement the decisions taken within the MARAC.

- ❖ **Safety Plans** - The key outcome of MARACs is to create safety plans that are customized to the individual needs of trafficking victims. These plans should include measures such as safe housing, medical care, psycho-social and legal assistance. As part of the safety plans, crisis management plans need to be developed to respond quickly to high-risk situations, such as the imminent threat of re-trafficking or violence against victims.

In order to ensure the seamless implementation of the safety plans, mechanisms to regularly monitor the progress of safety plans and adjust them are needed. Ongoing, follow up with victims to ensure their ongoing safety and well-being are crucial steps to ensure the appropriateness and effectiveness of the measures.

- ❖ **Stakeholders** - In order to include the key aspects relevant to the victims' security in the safety plan, participation from a wide range of stakeholders, including law enforcement, NGOs, community organizations, and international partners is needed. This broad engagement ensures a holistic approach to addressing human trafficking. Each participant needs to have

the authority to take decisions on behalf of their organisations with regard to resource allocation and legal basis.

In order to create a shared understanding of the phenomenon, in the field of Domestic Violence, shared trainings to MARAC participants on human trafficking, including recognizing signs of trafficking, understanding the legal framework, and responding effectively to victims' needs, have become a standard.

- ❖ **Role of technology** - To enhance the effectiveness of MARAC in fighting human trafficking, it's crucial to develop secure digital platforms that enable real-time communication and coordination among participants. These platforms should incorporate advanced risk assessment tools, such as predictive analytics and data visualization, to identify patterns and trends in trafficking cases (changing demography of the victims, trafficking routes, trafficking modus operandi, etc.). Additionally, providing online resources, such as chatbots, hotlines, and information portals, offer victims essential support services and guidance, making assistance more accessible and comprehensive.
- ❖ **Monitoring and Evaluation** - MARACs need to establish metrics to evaluate the effectiveness of their interventions in trafficking cases. These metrics can include the number of victims assisted, the reduction in risk levels, and the successful prosecution of traffickers.

In order to ensure victim centered justice and services, it is key to implement feedback mechanisms to gather input from MARAC participants, victims, and other stakeholders. This feedback can help identify areas for improvement and inform future strategies. MARACs should not decide measures without the consent of the victim.

Potential Benefits of MARAC in Human Trafficking

MARAC enhances coordination among various agencies and organizations, resulting in more comprehensive and effective interventions. By engaging multiple stakeholders, MARAC provides victims with holistic support that meets their physical, emotional, and legal needs. MARAC in turn provide the individual case workers with a peer-validated approach avoiding a silo-effect. The model's proactive risk assessment and monitoring processes are instrumental in identifying and mitigating potential risks, thereby preventing further harm and re-trafficking. Additionally, the collaborative approach facilitates the collection of evidence and ensures witness protection, leading to higher prosecution rates of traffickers. By involving community organizations and raising public awareness, MARAC can foster a more informed society, which helps reduce the prevalence of trafficking.

Challenges of MARACs

Adapting MARACs for human trafficking relies on the adequate allocation of resources, including funding, personnel, training and technology. It's crucial to ensure sustainable resource support to maintain the model's effectiveness. Participants require specialized training and expertise to navigate the complexities of human trafficking cases effectively. Furthermore, MARAC must be tailored to the cultural contexts of the communities it serves, guaranteeing that interventions are both respectful and appropriate. In addition, managing legal and ethical considerations are crucial; safeguarding the confidentiality and security of sensitive information is essential, necessitating the establishment and adherence to clear guidelines.

9 Child-Oriented Justice in Cases of Trafficking in Human Beings (THB)

Ensuring that child victims of THB receive appropriate protection and support is critical in justice processes. The following key aspects highlight the importance of child-oriented approaches in legal proceedings and cooperation among relevant institutions:

Special Protection Measures for Child Victims

- ❖ The Group of Experts on Action against Trafficking in Human Beings (GRETA) emphasizes the need for special protection measures for child victims of THB. This includes implementing the Council of Europe's Guidelines on child-friendly justice, which prioritize the well-being and rights of child victims during judicial processes.

Child-Oriented Questioning

- ❖ While criminal proceedings are typically offender- and offence-oriented, it is crucial to consider the specific needs of child victims to protect them and to accurately establish the facts. Child victims' statements often serve as key evidence in THB cases, and the reliability of this evidence can be enhanced through child-appropriate questioning techniques.

Specialized Training for Professionals

- ❖ **Training for Interviewers:** It is crucial to provide specialized training for individuals conducting interviews with child victims. This training should encompass developmental psychology,

trauma psychology, and memory psychology. Understanding these aspects is essential to address the unique needs of child victims, reduce trauma, and enhance the reliability and accuracy of the information collected.

- ❖ **Training for Judges and Law Enforcement:** Judges and police officers should also receive comprehensive training in these areas. This knowledge helps them better support child victims throughout the judicial process and ensures that child testimonies are handled with the utmost care and sensitivity.

Child-Friendly Facilities and Procedures

- ❖ **Establishing Child-Friendly Environments:** States should ensure the availability of child-friendly facilities at police stations and courts. These environments can significantly reduce the stress and anxiety experienced by child victims during interactions with the justice system.
- ❖ **Standard Guidelines for Interviews:** It is important to develop and implement standard guidelines for recording interviews with child victims. These guidelines should be tailored to protect the child's well-being and ensure that interviews are conducted in a consistent, respectful, and non-traumatizing manner.

Cooperation for Child-Oriented Justice

- ❖ **Inter-Institutional Cooperation:** Effective cooperation among various institutions, including law enforcement, social services, and child advocacy groups, is crucial for protecting child victims and ensuring comprehensive investigations. States should work to establish and strengthen these collaborative networks.

- ❖ **Addressing Regional Disparities:** Efforts should be made to reduce regional disparities in the development of cooperation structures. This includes ensuring that all regions have access to the necessary resources and support systems to protect child victims.
- ❖ **Networking Infrastructure:** Establishing a centralized structure for networking can facilitate formal cooperation and improve the efficiency of victim support services. This infrastructure should include clear protocols and channels for communication among all relevant stakeholders.
- ❖ **Data Protection and Resource Allocation:** States must clarify data protection regulations to enable effective information sharing while safeguarding the privacy of child victims. Additionally, adequate financial resources should be allocated to support these cooperative efforts and to raise awareness about the importance and benefits of networking and cooperation.

Assessment and Guidelines

- ❖ While recognizing that an ‘assessment catalogue’ or checklist can be too rigid for addressing the diverse needs of child victims, a well-prepared guideline can be helpful. Such guidelines should serve as a support tool, ensuring that all relevant factors are considered and that practitioners understand the purpose and importance of each inquiry.

By adopting these child-oriented justice measures, states can create a more supportive and protective environment for child victims of THB, ensuring that their rights are upheld and their well-being is prioritised throughout the justice process.

10 Using a victim-centric approach from investigation to prosecution

This manual addresses the critical role of digital tools and evidence in the fight against human trafficking. While investigative processes, technological tools, and legal frameworks form the backbone of modern efforts, effective strategies for supporting victims are equally essential. This chapter explains why a victim-centred approach is vital, explores foundational methods for working with victims, and outlines key strategies for the sensitive and ethical use of digital evidence.

10.1 Understanding the importance of working with victims

There are two main drivers for justice professionals to develop effective engagement strategies with victims. On the one hand under European and national law, victims of crime benefit from a range of rights, including those founded on human rights. The implementation of many of those are the direct responsibility of law enforcement and justice officials. This includes the right to information in an understandable manner, an individual needs assessment for protection and accompanying protection measures, interpretation and translation rights and facilitation of participation in criminal proceedings.

These rights are primarily focused on addressing the core needs of victims and are increasingly based on the understanding that our police and justice systems must be people focused. In other words, officials must not only seek to prevent crime and pursue criminals, but their role is also to help address the harm caused by crime or at least to minimise such harm when carrying out their duties. This role – of protection and support to victims within criminal proceedings – is a relatively new role for law enforcement and justice officials and continues to be embedded in the culture of organisations across Europe.

In addition to this legal and moral driver for addressing victims' needs in criminal proceedings, it is also well documented that 'getting it right' for victims is an important element in the success of any criminal investigation, prosecution and trial.

Their involvement is essential for gathering evidence and first-hand testimony of the crime. During the investigation and prosecution phase – victims provide **key details & insights** that guide law enforcement in identifying suspects, understanding the circumstances of the crime, and gathering corroborative evidence, building a prosecution case and helping the court to fully understand the consequences of the crime, potentially supporting a decision on sentencing. Their cooperation can significantly influence the direction of criminal proceedings, effectively making their role indispensable in building a strong case.

Where victims' rights are enforced, where they are treated respectfully and supported to participate, victims are more likely to continue with a prosecution and are better placed to give their best evidence. Without this approach, victims are reluctant to report crime, may withdraw their complaint, may struggle to provide useful information, may struggle to provide compelling evidence in court, and are more likely to drop out of the process and therefore jeopardise the case. Even without a focus on rights and well-being, it is therefore crucial to the effectiveness of an investigation, prosecution and trial that victims are treated in a proper manner.

For law enforcement and justice officials to be successful in combatting and prosecuting crime, they must be successful in working with victims. This means rooting actions in a right based, needs focused approach i.e., a victim-centric approach. The following sections aims to support officials in improving their engagement with victims through a victim-centric approach.

10.2 Fostering a victim-centric approach

According to the UN, a victim-centric approach is:

A way of engaging with victim(s) that prioritises listening to the victim(s), avoids re-traumatization, and systematically focuses on their safety, rights, well-being, expressed needs and choices, thereby giving back as much control to victim(s) as feasible and ensuring the empathetic and sensitive delivery of services and accompaniment in a non-judgmental manner

This definition provides core elements of a victim centric approach and should be at the heart of any process determining victims' policy, practices and laws, including how victims are treated within criminal proceedings.

At the same time, it is recognised that victim-centric approaches may need to be adjusted to take into account other priorities, balancing of obligations or limiting factors such as cost issues, defence rights, trial time frames, etc. A **victim-sensitive approach** builds on victim-centric solutions but subsequently adapts these to match with the criminal justice environment.

Victim-sensitive responses should ensure efficient justice systems, which are also flexible and adaptable to guarantee a targeted, individualised approach (VSE, 2023). Guided by such principles, national systems should be designed to **empower victims' participation** throughout proceedings, guaranteeing **respectful treatment, safety and prevention of repeat victimisation**, and the minimisation of harm at every stage of the process (VSE, 2023).

To adopt this approach, it is necessary to understand:

- ❖ how crime impacts victims

- ❖ what needs victims have
- ❖ what are the barriers to addressing these needs and rights (VSE, 2023).

11 The Aftermath of Crime: Impact and Needs of Victims

11.1 Impact of Crime on Victims & Society

The impact of crime on individuals can vary widely. Some may be affected to a limited extent. In fact, humans are for the most part very resilient to trauma and have good internal coping mechanisms, especially where they have a strong social support network of family and friends.

Supporting the victim's social network:

Family and loved ones can play a critical role in helping victims recover and participate in proceedings, whilst others may have the opposite effect.

When working with victims, it is useful to identify potential sources of support within a victim's network and explore how you can help them to be supportive of victims e.g., by accompanying victims at difficult moments (interviews, testimony), assisting with administrative tasks (filling out compensation forms).

They may struggle to know how to talk to a victim and be supportive. Identify materials, guidance and local resources that can help them. This can be particularly important for parents of child abuse victims. Many materials, groups and training exist to help parents understand what their child is going through and to learn how best to communicate and support them.

For others, crime – in particular, those classified as traumatic – can have severe consequences **extending far beyond the crime itself**. The days, weeks and months afterwards can be equally, if not more overwhelming, than the crime itself, leaving victims feeling helpless and unsure of the steps they need to take next (VSE, 2022).

IMPACT OF TRAUMA ON VICTIMS		
Immediate	Short term	Long term
<ul style="list-style-type: none"> ❖ Shock, surprise, and terror. ❖ Anger ❖ Emotionless, split personality ❖ Feelings of unreality, such as “This can’t be happening to me.” ❖ High rates of physiological anxiety (e.g., rapid heart rate, hyperventilation, stomach distress). ❖ Helplessness 	<ul style="list-style-type: none"> ❖ Preoccupation with crime (e.g., “I can’t get it out of my mind”). ❖ Flashbacks and bad dreams. ❖ Heightened concern for personal safety. ❖ Heightened concern for safety of loved ones. ❖ Fear they are at fault. ❖ Fear they will not be believed. ❖ Fear they will be blamed. ❖ Fear of law enforcement ❖ Inability to trust people/situation. ❖ Fear of the next attack. 	<ul style="list-style-type: none"> ❖ PTSD ❖ Depression. ❖ Alcoholism and substance abuse. ❖ Mental illness. ❖ Suicide (contemplation) ❖ Panic disorders. ❖ Obsessive-compulsive disorder. ❖ Poor health (e.g., physical disabilities, sexually transmitted diseases resulting from rape, immune system problems, developmental disabilities from a head injury). ❖ Chronic pain. ❖ Sexual dysfunction.

Table 6 – Impact of trauma on victims

Victims of crime often face a range of **physical injuries**, which can be both visible – such as cuts, bruises, and wounds, which are immediate and apparent – and internal – which may involve damage to organs, the brain, or other internal systems (VSE, 2023). These physical injuries can lead to long-term health complications, including chronic pain, impaired function, or permanent disabilities, all of which can contribute to a victim’s overall health burden.

The **psychological impact** of crime can be equally, if not more, devastating. Victims may experience severe emotional distress, including trauma and Post-Traumatic Stress Disorder (PTSD) (VSE,2023). This distress can manifest in various ways, such as anxiety, depression, and flashbacks. Trauma may result in memory loss, difficulties in processing and retaining information, or trouble recalling the events of the crime (VSE, 2023). Furthermore, psychological trauma can lead to behavioural changes, such as increased caution, withdrawal from social activities, or substance abuse. The emotional toll can also exacerbate existing mental health conditions or trigger new ones, creating a cycle of distress that can be challenging to break.

Victims who have experienced severe trauma, or repeated and prolonged victimisation often change their entire perspective on the world, their belief systems, their trust in others and their self-confidence and feeling of empowerment. Criminals, especially traffickers, will use many techniques to reduce confidence, increase fear and reliance on the criminals. All of these factors should be taken into account when speaking with victims. It makes **trust building, sensitive communications and victim empowerment** critical to successful engagement with victims.

Impact of trauma on victim response and memory:

When a person faces a serious threat, their body experiences physiological changes which are outside of their control. *Whether they resist or fight back, runaway, freeze or beg – these are automatic responses largely outside of the person's choice.*

The crime and the victim's reaction have an important impact on a victim's perception of themselves and their ability to cope with the trauma. *For example, a father who freezes during a burglary and is unable to help his family, may be burdened with feelings of guilt. Based on stereotypical expectations the family, community and even officials may also 'blame' the father for not acting with these reactions causing further trauma. The impact of the crime itself can leave victims with feelings of anger, shame, guilt. These reactions may be in the short term and can potentially remain and worsen in the long term. Not only is this detrimental to the victim and their family but also to their role in the criminal justice system.*

Officials can play a role in mitigating these impacts and supporting victims to participate in proceedings. *Through officials' own reactions, victim-sensitive communications, awareness raising of the victim and needs assessment and referral to support services, negative impacts can be greatly reduced.*

Trauma also impacts a victim's perception and memory of the crime which affects a victim's explanation of what happened during investigation and trial. *It is essential to understand these effects so that information is not dismissed or doubted, and so that where confusion or mistakes may be possible, this can also be checked.*

For example, in a threatening situation, a victim will focus on certain details and be completely unaware of others. E.g., not remembering any facial details but describing in detail an item of clothing or the weapon used. As such, simply because a person doesn't remember certain details doesn't now show the unreliability of a testimony or indicate the victim is hiding some information.

Similarly, the subconscious may fill in details which are missing from the memory without the victim consciously knowing this. Officials should take this into account where they identify discrepancies and not immediately assume a victim is deliberately lying.

These are just two examples of how trauma can not only affect victims personally but how that in turn can impact on an investigation. With a clear understanding of this, officials will be better equipped to both support the victim and to get to the truth.

Crime imposes a significant **financial burden** on victims – and consequently, to society. This burden can be both direct – for instance, medical expenses, such as costs for emergency care, ongoing treatment, and rehabilitation – or indirect – crime-related lifestyle changes, such as loss of employment, or forced withdrawal from education (VSE, 2023). The cumulative effect of these financial strains can lead to long-term economic hardship, impacting victims' quality of life and their ability to recover fully.

Crime further impacts the social life of individuals, with the potential of significantly altering a **victim's daily life and relationships**. Victims may experience social isolation due to fear, mistrust, or stigmatisation. This social withdrawal can further exacerbate feelings of loneliness and distress. The need for support from family and friends can be intensified, and the strain of providing such support can affect the wellbeing of those around the victim.

Understanding this, officials should be trained and have the tools to help mitigate the impact of the crime, support victims in their testimony and participation in proceedings and connect them to professional support services.

11.2 Needs of Victims in the Aftermath of Crime

The nature, type and impact of a crime have a direct influence on the needs of victims. However, many other factors such as the personal situation, history, and characteristics of a victim will also influence what their needs are.

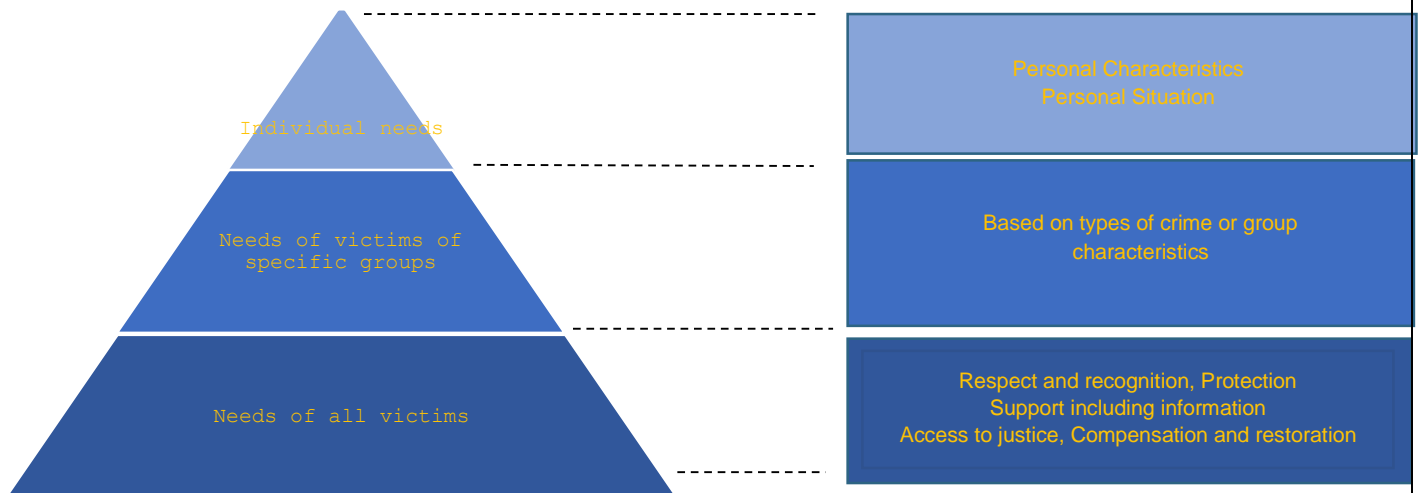
Many of these needs may relate to a victim's personal life whilst others may be specific to criminal proceedings or may be cross cutting through different aspects of a victim's life. These needs can be summarised as:

- ❖ the need to be recognised and treated with dignity and respect;
- ❖ the need to be protected from further victimisation and secondary victimisation;
- ❖ the need to be supported and receive understandable information;
- ❖ the need to access justice; and
- ❖ the need for compensation and restoration (VSE, 2023).

The better these needs are understood, the better they can be addressed. In doing so, the wellbeing of victims is improved and their ability to be effective participants in the justice process is increased – which in itself meets victims’ needs. This becomes a virtuous circle benefitting also those within the system.

Whilst this provides a good guide to common needs, no two victims are the same. As with changing impacts, needs also change depending on the type and nature of the crime, personal situation, history, and characteristics of each victim. Some factors may be common to certain groups based on e.g. which crime they have suffered, their religion, culture, sexual orientation, disability.

Figure 1: The Pyramid of Victims' Needs (VSE)



Responses must therefore be **tailored to fit each victim's specific circumstances**. This means having a menu of solutions and responses with some flexibility to allow for adjustments.

Thus, for example, some victims may need a protection order due to threats from the suspect. A range of orders may be available but only those most relevant e.g., a no contact order, may be requested. Other victims may not need a protection order but may be fearful of seeing the suspect in court. Special measures such as screens, separate waiting areas, and video testimony can be arranged.

Some solutions may be designed having in mind an entire group of victims. With respect to children, for example, there may be measures to facilitate interviews such as the presence of a psychologist, two-way mirrors to avoid large numbers present during the interview, use of a facility dog, and video testimony. Importantly, whilst those measures may be available, the victim should be involved in deciding whether they are necessary and used.

This means carrying out an individual needs assessment of all victims, at least for the purposes of physical protection and to prevent secondary victimisation. Ideally, the assessment would also determine wider needs and solutions to support participation in proceedings and access to rights.

In addition to understanding crime impacts and needs, it is also important to understand what barriers exist that prevent victims from accessing their rights and having their needs met. With this full understanding, appropriate, targeted solutions can be adopted.

The Five categories of victims' needs

Respect and Recognition *is fundamental to a victims' recovery to be recognised as victims and that their suffering needs are acknowledged. This idea not only concerns the treatment of victims by police and criminal authorities, but also their ability to rightfully participate and have a recognised voice during criminal proceedings.*

Support *needs encompass all forms of assistance victims need in the aftermath of crime. It can include a wide-ranging type of assistance – such as emotional, psychological, financial, legal or practical support -, which can involve multiple stakeholders over a long period of time.*

After a crime, victims often have a variety of protection needs which should be catered for. It can be both physical protection from harm/fear of further criminal acts by the offender, or protection from instances of secondary victimisation caused by behaviours, reactions and attitudes of stakeholders/the wider society interacting with the victim.

Access to justice *not only refers to the judgement itself, but also a victims' capacity to participate in criminal proceedings. It includes the ability to report a crime, the accessibility of court processes, and the ability to exercise rights & have a certain degree of influence within proceedings.*

Compensation & Restoration, *which address financial harms as well as the need for wider social recognition. In addition to financial compensation from the offender or the state, restitution may not solely be focussed on financial reparations but could include other forms of recognition such as an apology or community service.*

11.3 Barriers to accessing needs and rights

As a result of the multi-faceted impact crime poses on individual victims, their **engagement with practitioners & authorities can be hindered**. Their experiences of fear, disempowerment, and confusion can create numerous barriers, making it difficult for them to participate fully throughout proceedings (VSE, 2023).

Victims who are deeply traumatised may find it **overwhelming to navigate the complexities of the justice system**. Their belief systems (in particular in a safe, just world) can be damaged and they may come from a background where there are poor relations with authorities or criminals may have created a fear of police involvement. The net result is that victims may be highly distrusting of police and justice authorities.

This can manifest in a reluctance or outright refusal to come forward and report the crime. In some cases, victims may even struggle to accept or recognise that a crime has been committed against them, leading to delays in seeking help or cooperating with authorities (VSE, 2023).

Even when victims do engage with the system, their **trauma can hinder their ability to provide clear and consistent testimony**. They may struggle to recall details accurately, express themselves coherently, or maintain the emotional strength needed to endure examinations (VSE, 2021). The stress and anxiety associated with court appearances and legal proceedings can lead some victims to withdraw entirely, resulting in dropped cases or weakened prosecutions.

Further, **testifying** about the crime can be an overwhelming experience for victims, and the **emotional toll** it takes may result in fragmented testimonies. Trauma-induced behaviours – such as difficulty in recalling events, emotional outbursts, or apparent detachment – can be misinterpreted by professionals as a lack of credibility or cooperation, hindering the experience of victims.

The act of discussing the crime in detail can be **re-traumatising** for victims, especially if they are not provided with appropriate psychological support. The legal process can feel disempowering and intrusive, stripping victims of the control they need to regain in the aftermath of a crime.

Not only may the process be disempowering but the crime and victims' treatment by perpetrators can result in a loss of confidence and disempowerment leaving victims reluctant to express wishes and needs. They may want a support person to accompany them, they may be fearful of speaking in the presence of the perpetrator, or they may simply have not understood a question – yet they never mention any of this.

Proactive provision or offers of assistance, reminders of rights and multiple opportunities to access information or assistance are therefore essential.

12 Engaging effectively with victims of crime: a guide for practitioners

The advent of digital technologies has revolutionised the way evidence is collected, analysed, and presented in criminal investigations. Having in mind impact, needs and barriers, we focus on four key issues:

1. Rapport, trust, effective communication
2. Safety, privacy and transparency
3. Empowerment
4. Support

Following this victim centric approach will support law enforcement and justice practitioners to identify, obtain, handle, and present digital evidence in an efficient and legally sound manner whilst also maximising the care of victims and addressing their needs and rights.

It is important to understand that whilst the focus of this manual is on digital and online evidence and how you can best work with the victim to obtain this evidence, the most essential elements to success are relevant to all engagements with victims whether relating to digital evidence or not.

12.1 Building trust and rapport

Victims, in particular, victims of sexual abuse and human trafficking are often fearful and distrusting of authorities. The nature of the crimes, control and fear established by perpetrators and the vulnerable, often isolated situation of the victims who may be in a foreign country, reduces their willingness to cooperate and be open.

Officials consistently recognise the need to build and maintain rapport and trust with victims in order to facilitate any subsequent investigative actions. **Rapport can be described as agreement, mutual understanding, or empathy that makes communication possible or easy.** It enables people to connect, share feelings and establish communication with each other.

Relationship and rapport building techniques should be used whenever in contact with a victim to support victims and to improve cognitive processes, such as episodic memory (i.e., memory of everyday events). Comfortable witnesses will be more cooperative and better able to recall events, thereby increasing the accuracy of the interview (Nahouli, 2021). Yet there is often little focus on how such rapport should be developed.⁹

⁹ There are many frameworks for rapport building that should be explored e.g., Tickle-Degnen and Rosenthal model focused on mutual attention, positivity, and co-ordination with the other person; <https://psycnet.apa.org/record/1992-01371-001>

When considering approaches to rapport building, some of the key issues to consider are:

- ❖ **Environment:** when speaking to or meeting with a victim, a calm, safe and confidential environment helps stabilise the victim and focus on the conversation without fear.
- ❖ **Empathy and connection:** before focusing on questions about the crime, focus on the victim - their background, their immediate needs and concerns. Showing an interest in the person rather than only their victim status helps connect and build trust. Empathy, however, is not just about listening and putting yourself in their shoes, it's also about acting where you can.

The three core components of empathy:

Curiosity – *understand and focus*

Reflect back *the message*

Act on your understanding: *Address victims needs*

- ❖ **Effective communication:** this requires not only an understanding of what to communicate but also how to communicate. It is important to remember that communication is a two-way process. In other words, it's not only about what you want to communicate, it is also about listening to the other person. Some of the key communication skills to develop include:
 - ✓ **Active listening** – listening, understanding, confirming this is correct and responding appropriately.
 - ✓ **Trauma-informed communications** – interactions should be based on empathy, acknowledging the victim's pain and validating their experiences (Victim Support, 2023). Speaking to the victim in a non-judgmental, empathetic manner, confirming

they have understood, and recognising that what a victim says will be influenced by their trauma. Their words don't necessarily reflect what they are thinking or needing. In this respect, your tone and the tone of the victim are important communication tools.

- ✓ It is important that the victim perceives that they are believed and treated with dignity. The treatment of victims must be respectful and must reflect the notion that their words are taken seriously, properly recorded and investigated (Victim Support, 2023). Practitioners working with victims should operate under the assumption that an act of victimisation has occurred, if that is what the victim reports – victims should never be made to feel that they were not victimised nor that it was their fault (Victim Support, 2022).
- ✓ **Non-verbal communication:** body language, facial expressions, the clothes worn are all ways of communicating. Not only must you be aware of how you are communicating non-verbally, but you must focus on a victim's non-verbal communication and use this as a tool to understand the true thoughts and feelings of a victim. For example, a child may not directly object to a parent being present when digital evidence found on their phone is discussed. However, they may change their facial expression, tone, or body posture indicating concerns. Recognising this and interviewing the victim in another way e.g., parent's not present, or in a different room, can help illicit information that the victim may not otherwise provide.

Actions for and during an interview

Ensure a comfortable, safe and confidential environment: *Support the individual in feeling physically comfortable; for example, offer them water, show them where the restrooms are located, and periodically ask if they need anything. If not local, familiarise yourself with the interview room is important so you can describe what is in the room e.g., cameras, two-way mirrors, where the toilets are.*

Introductions: *be polite and friendly, introduce yourself, clarify your role and the purpose of the interview, ideally avoid wearing a uniform, use the victim's name, but check how they would like to be called. Provide reassurance. Build credibility: e.g., by explaining your years of experience in the job, or specifically on human trafficking.*

Be transparent and set ground rules: *discuss truth and lies, and the importance of honesty. Provide concrete and clear instructions, set expectations for the interview. Ask children to say "I don't know" or "I don't remember" rather than guessing and tell children to correct an interviewer when they say something wrong.*

Learn about the victim: *focus on their day-to-day needs and concerns, health, safety and support. Learn about the individual's background, risks and restrictions. Learn about their likes, hobbies, which are not associated with the crime. Find areas of commonality. E.g., what do you like to buy when you go shopping, who's your favourite sports person?*

Reassure the victim: *Reassure victims that they are respected and not held responsible for the crimes that occurred. Reassure them also about their legal situation, and other rights such as non-prosecution and no obligation to cooperate.*

Be aware of your verbal and nonverbal cues; *maintain a calm tone, eye contact, a warm, neutral facial expression and open body posture. Respect personal space and avoid personal contact unless discussed beforehand. Remain at eye level as much as possible.*

Monitor the victims' verbal and nonverbal cues for signs of physical or emotional discomfort. *By matching and mirroring the victim's pace, body and verbal language you will create a subconscious connection.*

Personal Behaviour tips

Be positive and give the victim credit: *they may have no one that recognises their strengths and qualities. By the time they meet you, they have probably suffered trauma and violence. They may be resilient and independent or lacking in confidence. Many will not recognise they are victims or not want to be treated like victims. Find opportunities for positive encouragement, respect and empower them to make their own decisions, whilst recognising this when they achieve it.*

Be patient and consistent: *victims will take time to build trust, to reduce fears, to remember and to be ready to talk about their experiences. Let them know that you are there when they are ready. In an interview, victims may struggle to find the words, may blank, or may be going through a difficult moment. You don't have to fill in the silences or give answers. Sometimes, victims just need time and space. Be consistent in what you say and do, inconsistency breaks trust.*

Be yourself: *Youth know when you are faking, and it can impact your credibility. DO educate yourself about the dynamics and language of CSEC; DON'T misrepresent who you are and where you've been.*

Be non-judgmental: *victims of abuse and human trafficking often feel ashamed, and may have been forced to do things against their will including commit crimes and take drugs. In your discussions with victims, non-judgement on their choices during the crime and also during the proceedings should be shown. If a victim says they don't want to give access to a social media account, judging them will not help. Supporting them to feel safe in providing access, to not feel judged, will help.*

Be kind: *Potential victims of trafficking may be belligerent or hostile. Their life experiences and past traumatisation make it difficult to trust care providers or people in authority.*

Maintain appropriate boundaries: *Make sure that the relationship you are building is healthy for both of you. Survivors should not depend on you to meet all of their needs, and you should not feel solely responsible for their well-being. Work with other community partners to develop a network of support for the survivor and yourself.*

Communication tips

Keep explanations simple but don't talk down to victims e.g. *"You will be audio and video recorded... my partner will be writing notes while I speak... you can stop the interview at any time."* Don't assume the level of a child's understanding. Repeat back or paraphrase what the victim said, to confirm understanding. By doing so, you should find the right level to communicate at.

Identify emotions of victims e.g. *"It seems to me that you are upset?"* Be sensitive to potential triggers that might remind a patient/client of past trauma. Be empathetic to their situation: *"I can understand why you might feel angry"*

Find points or phrases of agreement: *'yes exactly'; I know what you mean.*

Don't pressure the victim to answer questions if they hesitate - *giving them the space, control and discretion with what to disclose and how quickly; Suspect-focused techniques such as stressing the seriousness of the crime or the duties and obligations of the victims, does not tend to result in openness and cooperation. Offer the victims regular breaks.*

Ask for an initial open-ended narrative from victims and pose open-ended questions *circling back to the topic of trafficking. Encourage the processing of feelings, experiences, and choices. If they aren't ready to share with you, give them an opportunity to ask you questions.*

Information:

Practitioners should provide clear, straightforward explanations of rights, services and legal procedures, avoiding jargon that might confuse or overwhelm victims.

It can be hard for victims to concentrate for a longer time therefore they should be offered complex information in short and clear pieces of information whilst getting the chance to take a break in between if they want to. The difficulty of processing large amounts of complex information should not refrain the practitioner or law enforcement officer from giving all required information. If victims want to receive information, it is important to provide them with all necessary information in a simple, concise, accurate and transparent manner so that they can make informed decisions.

Practitioners should be ready to repeat the information, if the victim's experience difficulties in concentrating.

High levels of arousal at the time of seeking support or reporting a crime might hinder victims understanding the message of information given. Check with the victim to determine whether all information is understood or whether they would like it to be repeated. Don't just ask if they have understood, ask follow-up questions and review information together. Pose open questions about the issue. E.g., So where would you go to login into your account? Which of the leaflets has the information about compensation in it?

Victims should be given information in multiple formats – orally, in writing (leaflets, documents), digitally and through multimedia (interactive information, videos and presentations, infographics). In high stress situations, visual information might be easier to understand.

Establish digital solutions to help victims communicate and access information: digital technologies are an important tool in facilitating communication and collaboration between victims, law enforcement, and legal professionals. For instance, online portals or mobile applications can help victims to report crime and manage their digital evidence securely. This digital communication can also keep victims informed about the status of their case, providing them with updates and allowing them to engage more fully in the justice process.

12.2 Safety, privacy and transparency

For the victim's safety and to maximise your ability to interview the victim and obtain as much useful information as possible, it is essential to ensure the victim feels, and is in fact, safe.

A specialised **needs and risk assessment process** for human trafficking cases should already be in place. However, this may be a basic checklist without a focus on specific risks and mitigations arising from online crime. These should be incorporated into a risk assessment process.

The needs and risk identification process relies heavily on communication and empathy skills, particularly when working with children. A knowledge of the general situation of victims of human trafficking coupled with effective enquiry into the situation of each victim is essential.

The assessment should result in a safety plan with protection measures, strategies for avoiding or reducing the threat of harm and concrete options for responding when safety is threatened or compromised. Safety planning involves helping individuals anticipate and plan for potentially escalating levels of danger before, during, or after leaving a dangerous situation.

Risk assessments should focus not only on physical safety but also on fears about privacy, involvement in the proceedings, concerns about the safety of family members etc. Transparency is key for victims to have trust that they can report safely and co-operate with justice agencies. Officials should take a step-by-step approach when explaining complex procedures.

It is important to explain to or train victims in digital cleanliness and security. If they continue to access devices or accounts, these could be compromised or could result in perpetrators identifying them or their location. They may be used to intimidate victims or victims may purposely or accidentally delete important information.

Potential ways in which victims' communication channels may be compromised:

- ❖ traffickers have access to account credentials directly;

- ❖ physical access to clients' devices (including impersonating the client over the phone to monitor their contacts);
- ❖ installing tracking location devices & apps on their communication devices and/or vehicles;
- ❖ monitoring victims' online activity to identify their location;
- ❖ traffickers may also be present in the proximity of the building providing different types of services to victims to monitor the ins and outs and/or to recruit; they may also send a victim into a survivor program to recruit others directly.
- ❖ victims' have in their friend networks individuals who are still being exploited by traffickers and with whom they may be in contact.

Preserving contact with victims:

- ❖ Practitioners should make technology-related choices to protect victims from re-victimisation and other harm; This means assisting clients lock down social media accounts, and restricting their social media activity (e.g., to prevent their location from being identified).
- ❖ Practitioners must also acknowledge there may be instances where the only reliable communication with the victims can occur via trafficker-compromised accounts and platforms. In this case, balance must be achieved between building client trust and maintaining contact with imposing technology-related safety rules.
- ❖ No one-fits-all approach to technology security. While it is recommended that victims avoid sharing their location (including by disabling their location on mobile devices) and apply robust information security practices (e.g., changing their social media accounts; and constantly changing their passwords), there are a number of factors which play into technology use: e.g., age, technology-savviness, access to alternatives (Chen et al, 2019).

Advantages and disadvantages of different means of communication:

- ❖ Texting – this is often avoided (voluntarily and involuntarily) by trafficked victims due to concerns about (1) law enforcement confiscating phones and searching text messages; (2) identity of interlocutor - with texting, there is no authentication ensuring that you are communicating with the person you think you are communicating with.
- ❖ Phones have the advantage of enabling authentication, but they pose a higher risk for victims when they are still in a dangerous situation (e.g., the risk of being overheard). Moreover, phones can still be intercepted and phone call records monitored.
- ❖ Social media accounts – they are a very popular way for victims to communicate with victim support entities. Their main advantage is consistency (e.g., they can be used even when victims must switch devices or phone numbers or do not have credit to make a call provided there is internet access). Moreover, victims can employ apps which support end-to-end encryption and automated message deletion which can also help them hide these interactions from the traffickers. A number of these apps also hide their purpose – for example by appearing to be a shopping app. The true purpose is only identifiable through a secondary pin.
- ❖ Email is not popular, mainly due to lack of access and difficulty authenticating.

Privacy Legal and skills framework

There should be a proper legal framework regulating victims' rights regarding digital evidence. *Effectively, this should aim at protecting the right to privacy of victims, connecting it with the procedural rights already enshrined in legislation. This should also include the right to receive information about their case, the right to access their data, and the right to challenge the use of digital evidence in court.*

Cases should be handled with the utmost integrity, considering the role of victims and the impact the digital evidence may have on them. *Digital technologies have given rise to a new set of crimes which requires not only having an appropriate legal framework but also providing training and ensuring officials have relevant qualifications.*

Above all, evidence should be collected in an ethical manner. *Regardless of the value of the information extracted, investigators should seek to safeguard as best as possible the victim's human rights. For example, any privacy invasions should be minimised, avoiding the exposure of personal information which can potentially threaten their safety.*

Concerning access to digital evidence, understanding victims' concerns about providing access to devices and accounts and discussing options for how privacy may be protected will help reassure the victim and increase the likelihood they will provide access and be open about all their online accounts. In collecting such data – especially if the data comes from personal devices or social media accounts – victims should be fully informed about how that digital information will be used. When working with children, explain what the role of parents or legal guardians will be when accounts/ phones are accessed and take into account their concerns in this respect.

In some cases, victims may feel hesitant to come forward or be open due to fears of not being believed or of facing retaliation. Yet, digital evidence helps to **enhance the credibility of victims' statements**. You should therefore explain to victims how digital evidence will support their claims and support a successful investigation and prosecution. This can help victims to feel more confident in reporting the crime and participating in the investigation.

One important component of a victim-centric approach to prosecution is providing victims from criminalization – often achieved via ‘safe harbour’ – type legislation.

Tips on access victim data

Aim for as minimally intrusive approach as possible. *Ensure you have consent of the victim (wherever appropriate) and if appropriate obtain this in writing.*

If data can be obtained without taking devices this is ideal. *Where a device needs to be taken, minimise the amount of time it is held for. Help victims to transfer essential data onto alternative devices to minimise the loss of devices.*

Reassure the victim about how devices and accounts will be used, *who will have access to etc. Try to minimise the number of people accessing data, in particular data which is not relevant to the case. Establish time limitations on access.*

Discuss with the victim if there is personal information not relevant to the case which they don't want officials to see. *Explore how to protect this data (e.g., victim places it in a secure folder) or further limit who sees the data and where it is recorded or kept. Limit the holding of data for evidence to that which is strictly necessary for the case.*

Using technologies that can anonymise or redact sensitive information *in the digital space can help protect victims while still allowing the evidence to be used effectively.*

Discuss any 'safe harbour' provisions *there may be in place, and which should be considered when collecting & analysing digital evidence to be found on the victim. There are different approaches which can be employed ranging from using digital evidence to substantiate the victim's lack of control; to using discretionary powers to not proceed with criminal charges when the digital evidence points to potential criminal acts carried out by the victim but instead directing trafficking victims to support services. Finally, where charges are filed, some jurisdictions offer diversion programs that replace traditional prosecution with alternative programs including treatment, education and support options.*

There are also several measures which can be taken to prevent re-victimization via exploitation of digital evidence in a court setting.

- a. Not requiring judges to view digital evidence at sentencing (e.g., UK) - this measure is adopted to both mitigate re-exploitation, re-traumatisation and stigmatisation of victims; as well as preserve the mental health of the courts. In these situations, judges are provided with a description of the evidence-based on CAID categorisation (categories A, B and C)¹⁰.
- b. In some jurisdictions, judges decide who attends sessions where such evidence is being shown.
- c. Only a selection of material is shown during criminal proceedings (e.g., Sweden).

The disadvantage of this approach of not viewing fully the digital evidence may result in an underestimation of the crime and the harm it causes (ECPAT France, 2022).

12.3 Empowerment and support

A major factor in the trauma victims experience is the loss of control and feeling of powerlessness arising from the crime. It is therefore important to empower victims through any engagement with them. Two main ways to achieve this are by **providing victims with information and skills**, and by **giving them choices**.

¹⁰ category A – images involving penetrative sexual activity, sexual activity with an animal or sadism; category B – images involving non-penetrative sexual activity; and category C – other indecent images not falling into categories A or B, but it must not depict any sexual activity.

This can be particularly important when working with children as it may be natural to assume the child can't do something, doesn't understand or is unable to make decisions. However, in many cases, it is a question of supporting the child to understand or to make a choice.

As mentioned above, explaining to a victim what will happen, what procedures will be followed, what rights they have and how to access those rights is extremely important. Information can quickly move from being helpful to being overwhelming.

If a victim appears confused or unable to decide or take action, explore where the difficulty lies. Help the victim to identify options and understand the consequences – advantages and disadvantages of any action.

For example, if a victim is concerned about private images being shown in a public court, help them to understand who will be present, and what options to limit presence exist e.g., an order for the public to be removed, or certain people such as family members to not be present, restriction of viewing to only certain individuals, absence of the victim during showing etc.

Be clear when a victim has a choice. It is important to present all available options and their potential, allowing victims to make decisions that align with their needs and expectations from proceedings. For example, whether to provide certain information or not. Whilst pressuring a victim may get a quick result it can break trust which can ultimately reduce the likelihood of a successful case. Respecting the decisions victims make – choosing to participate or not – reinforces their autonomy and promotes their sense of control and dignity.

As much as possible, where you must make decisions that affect a victim e.g., protection orders, referral to services, and involve the victim in the process and the decision. You may feel that a young person should give testimony via video link to protect them from seeing the perpetrator again.

However, they may want their 'day in court' - to stand up and show the perpetrator they are not fearful. Discussing what the victim wants as well as any procedural, legal or safety concerns you have, will help build trust and also find the best solution.

Recognise your limitations. You will not always be the best person to empower a victim. Ensure they have the appropriate support services and legal assistance. Victims may be accompanied by a loved one during interviews. They may benefit from a professional support service or a lawyer to help them make decisions.

Remember, victims often don't want to be a burden on the system. They may say they don't need support if first asked. Keep checking with them and ideally have a referral system in place so that support services can directly explain to the victim how they can help.

To maximise access to appropriate support:

- ❖ **Establish a support referral mechanism.** Ideally, this is a mandatory, opt-out system which means that victims are informed their information is passed on to support services, unless they object. The support service will contact the victim directly to explain their work and offer assistance. This is the most effective mechanism for enabling access to support.
- ❖ **Ensure multiple support solutions exist:** external support service for all needs (including e.g., shelter), in-house support services (e.g., police psychologist), support in court, court accompaniment, accompaniment by loved one, legal assistance etc.
- ❖ **Remember that victims need change over time** and victims don't always understand or know they need support. Check regularly if victims would like support.
- ❖ **Be aware of all local services and ensure effective coordination arrangements exist.** Even if not local, ensure you have connections with services specialised in handling online crime –

whether the organisation deals only with such crimes or if an all crime (generic victim support) if they have in-house specialisation.

- ❖ **Remember you are part of the support system.** By following the basics of psychological first aid, active listening, empathy and effective communication, you will already be operating in a supportive manner.

12.4 Compensation for Victims of Trafficking in Human Beings (THB)

Compensation for victims of THB is a crucial aspect of justice and rehabilitation, providing victims with financial redress and helping to address the harm suffered. Various practices and recommendations emphasize the need for effective mechanisms to ensure that victims receive appropriate compensation.

To provide effective access to compensation for victims of THB, states should adopt the following general guidelines:

Comprehensive Evidence Collection

- ❖ Criminal investigations should thoroughly document the harm suffered by victims and the financial benefits accrued by traffickers. This includes gathering evidence such as medical reports, witness testimonies, and financial records. Comprehensive evidence is crucial in supporting compensation claims in court, ensuring that victims can substantiate their losses and receive appropriate restitution.

Proactive Prosecutorial and Judicial Action

- ❖ Prosecutors should systematically seek compensation for victims as part of the prosecution process. This involves formally requesting compensation during trials and highlighting the

impact on the victims. Judges, in turn, should use all available legal mechanisms to uphold these claims. This proactive stance helps make compensation a routine and integral part of judicial outcomes, reinforcing the accountability of traffickers.

Establishing Legal Procedures for Compensation

- ❖ States should introduce specific legal procedures that allow victims to obtain compensation decisions from offenders within the framework of criminal trials. This could include provisions for courts to automatically consider compensation as part of sentencing. Furthermore, if compensation is not awarded, courts should be required to provide a clear explanation for this decision, promoting transparency and accountability in the judicial process.
- ❖ Training for legal professionals should also be regarded: Additional training for prosecutors and judges on the issue of compensation is recommended. This training would focus on the importance of compensation for victims' recovery and the legal mechanisms available to secure it.

By implementing these guidelines, states can create a more robust and victim-centred approach to compensation in THB cases, ensuring that victims receive the financial redress they need for recovery and rehabilitation.

Local and Regional Promising Practices:

1. **Swedish Crime Victim Fund:**

- ❖ In Sweden, a unique model involves a Crime Victim Fund, managed by the Crime Victim Compensation and Support Authority. The fund is financed primarily through contributions from convicted offenders, amounting to approximately €3.5 million annually. This fund

supports victim services and projects, providing a consistent financial resource for victim support.

2. **Compensation Orders in the UK:**

- ❖ In the United Kingdom, compensation orders are imposed by criminal courts as part of the sentencing process. These orders focus on reparations based on the victim's loss and the offender's ability to pay. Unlike civil claims, compensation orders are integral to the criminal justice process, and non-compliance can lead to further sanctions against the offender. This ensures that compensation is not only punitive but also restorative.

3. **The Advance Payment System in the Netherlands**

- ❖ In the Netherlands, among the various forms, victims of human trafficking can be compensated, through the criminal proceedings in which the (alleged) human trafficker is prosecuted. The victim may join these proceedings and submit a claim for damages. In addition, the court can impose a compensation measure. Compensation is regularly obtained in criminal proceedings and, since the introduction of the advance payment system, this is also the most secure method. Based on the advance payment system, the state guarantees payment of the compensation measure, meaning that the victim is not personally responsible for execution.

Effective access to compensation is vital for the recovery and rehabilitation of victims of trafficking. The integration of compensation mechanisms into criminal proceedings, proactive legal action by prosecutors and judges, and state-backed advanced payments are essential measures. Additionally, models like Sweden's Crime Victim Fund and the UK's compensation orders highlight innovative approaches to ensuring that victims receive the financial restitution they deserve. These practices not only support victims but also reinforce the accountability of traffickers.

Bibliography

- ❖ Abdi, Feven. Understanding Cybercrime through the Lens of Victim Experiences. 2023. Available at: <https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1057&context=covacci-undergraduateresearch>
- ❖ Akhgar, B., et al. Online Child Sexual Exploitation: A New MIS Challenge. Available at: https://www.academia.edu/69176459/Online_Child_Sexual_Exploitation_A_New_MIS_Challenge
- ❖ ASEAN Do No Harm Guide for Frontline Responders: Safeguarding the rights of Victims of Trafficking in Persons. <https://acwc.asean.org/wp-content/uploads/2024/06/ASEAN-Do-No-Harm-Guide-Capacity-Enhancement-of-Frontline-Responders-in-Countering-Trafficking-Using-Victim-Centred-and-Gender-sensitive-Approaches.pdf>
- ❖ Article 3 (1) REGULATION (EU) 2023/1543 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2023.
- ❖ Article 3 (2) REGULATION (EU) 2023/1543 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2023.
- ❖ Article 3(1) REGULATION (EU) 2023/1543 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2023.
- ❖ Article 14(1) & (2)(c).

- ❖ Article 3 of Directive 2011/92/EU.

- ❖ Article 4 of Directive 2011/92/EU.

- ❖ Article 5 of Directive 2011/92/EU.

- ❖ Article 6 of Directive 2011/92/EU.

- ❖ Article 7 of Directive 2011/92/EU.

- ❖ Barlow, D. H., Clinical handbook of psychological disorders: a step-by-step treatment, UK: The Guilford Press, 2002. Quoted in Communicating with Victims: A Handbook for Officers; p6; <https://victim-support.eu/publications/handbook-for-officers-communicating-with-victims-of-crime/>

- ❖ Caring for Trafficked Persons: Guidance for Healthcare Providers. <https://publications.iom.int/books/caring-trafficked-persons-guidance-health-providers>.

- ❖ Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press, 2011.

- ❖ Chen, Christine, et al. "Towards Detecting Malicious Behaviors in Crowdsourced Live Video Streams." Computers in Industry, 2022. Available at: <https://www.sciencedirect.com/science/article/pii/S0950705122011327>

- ❖ Chen, Christine. "Detecting Malicious Behavior in Cybercrime." *Computers in Industry*, 2022. Available at: <https://www.sciencedirect.com/science/article/pii/S0950705122011327>
- ❖ Chen, Christine, et al. *Protecting Against Predators: Full Report*. Available at: <https://www.drugsandalcohol.ie/39025/1/Protecting-Against-Predators-FULL.pdf>
- ❖ Collins, R. et al. **The Effect of Rapport in Forensic Interviewing**. https://pure.bond.edu.au/ws/portalfiles/portal/27325535/2002_The_effect_of_rapport_in_forensic_interviewing.pdf
- ❖ Council of Europe. *Online and Technology-Facilitated Trafficking in Human Beings: Full Report*. Available at: <https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49https>.
- ❖ Crown Prosecution Service. *Social Media: Reasonable Lines of Enquiry*. Available at: <https://www.cps.gov.uk/legal-guidance/social-media-reasonable-lines-enquiry>
- ❖ European Commission. *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1543>
- ❖ European Union Agency for Criminal Justice Cooperation. **SIRIUS Platform: A Secure System for Communication and Information Exchange. * Eurojust*.
- ❖ Europol. *How Not to Fall for the Lover Boy Scam*. Available at: <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/how-not-to-fall-for-lover-boy-scam>.

- ❖ Directive (EU) 2011/92/EU on Combating the Sexual Abuse of Children. Available at: <https://eur-lex.europa.eu/eli/dir/2011/92/oj>

- ❖ Fernando Molina Granja; Glen D. Rodríguez Rafael International Journal of Electronic Security and Digital Forensics (IJESDF), Vol. 9, No. 1, 2017

- ❖ *Fight Against Terrorism – Definitions of Terrorist Crimes and Support to Victims* (2018), available at: Directive (EU) 2017/541 of the European Parliament and of the Council. (europa.eu).

- ❖ Gagnon, K., & Cyr, M. *Sexual Abuse and Preschoolers: Forensic Details in Regard of Question Types*. <https://www.nationalcac.org/wp-content/uploads/2016/10/Sexual-abuse-and-preschoolers-Forensic-details-in-regard-of-question-types.pdf>

- ❖ Government of Canada. *Trauma-Informed Police Resources for Human Trafficking Cases.* *<https://www.justice.gc.ca/eng/rp-pr/jr/tiprhtc-rptctctp/index.html>

- ❖ Hendrix, J. (2024, October 6). Unpacking new Mexico's complaint against snap inc. Tech Policy Press. <https://www.techpolicy.press/unpacking-new-mexicos-complaint-against-snap-inc/>

- ❖ Human Rights, Gender Sensitive and Child-Friendly Approaches to Trafficking in Persons Cases for Frontline Officers. <https://aichr.org/wp-content/uploads/2023/07/AICHR-Training-Manual-on-Human-Rights-Approaches-to-TIP.pdf>

- ❖ Human Trafficking: What to Do? *A Practical Guide for Healthcare Providers, Law Enforcement, NGOs & Border Guards. * <https://www.payoke.be/wp-content/uploads/2019/05/Guide-For-Practitioners.pdf>
- ❖ ICMPD. Law Enforcement Manual to Combat Trafficking in Human Beings. Available at: <https://www.icmpd.org/file/download/54287/file>
- ❖ Interactions Between Victims of Intimate Partner Violence Against Women and the Health Care System: Policy and Practice Implications. <https://journals.sagepub.com/doi/abs/10.1177/1524838007301220>
- ❖ Kirkner, A. C., et al. "Challenges in Addressing Sexual Violence and Human Trafficking Using Multidisciplinary Approaches." Violence and Gender, 2020. Available at: <https://www.liebertpub.com/doi/abs/10.1089/vio.2020.0105>
- ❖ Lariviere, C. et al. *The Effects of Rapport Building on Information Disclosure in Virtual Interviews.* <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9281184/>
- ❖ Latonero, M. *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds.* University of Southern California Annenberg School for Communication & Journalism, 2011.
- ❖ Lavorgna, A., et al. "Policing the Dark Web: Lessons Learned from Cybercrime Investigations." Policing: A Journal of Policy and Practice, 2019. Available at: <https://academic.oup.com/policing/article/15/1/68/5250859>

- ❖ Macias-Konstantopoulos, W., et al. *Adult Human Trafficking Screening Tool and Guide: A Guide for Training Public Health, Behavioral Health, Health Care, and Social Work Professionals*https://nhhtac.acf.hhs.gov/sites/default/files/2018-07/adult_human_trafficking_screening_tool_and_guide.pdf

- ❖ Molina Granja, Fernando, & Rodríguez Rafael, Glen D. *The Preservation of Digital Evidence and Its Admissibility in the Court*. *International Journal of Electronic Security and Digital Forensics** (IJESDF), Vol. 9, No. 1, 2017.

- ❖ Nahouli, Z. et al. *Rapport Building and Witness Memory: Actions May ‘Speak’ Louder Than Words*. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0256084>

- ❖ National Human Trafficking Training and Technical Assistance Center. *Trauma-Informed Care*. https://nhhtac.acf.hhs.gov/soar/eguide/respond/Trauma_Informed_Care

- ❖ Nelson et al. *Interacting in Flow: An Analysis of Rapport-Based Behavior as Optimal Experience*. <https://core.ac.uk/download/pdf/83896357.pdf>

- ❖ Nexus Institute. *Supporting the Reintegration of Trafficked Persons: A Guidebook for the Greater Mekong Sub-Region*. Available at: <https://nexusinstitute.net/wp-content/uploads/2017/04/final-reintegration-guidebook-gms.pdf>

- ❖ Oerlemans, J. J. *Cybercrime Investigations*. Available at: https://www.researchgate.net/publication/357302986_Cybercrime_investigations

- ❖ Organization for Security and Co-operation in Europe (OSCE). Trafficking in Human Beings: Identification of Potential and Presumed Victims – A Community Policing Approach. Available at: <https://www.osce.org/files/f/documents/4/e/78849.pdf>

- ❖ Policy Guide on Protecting Victims of Trafficking: *An Introductory Guide for Policy Makers and Practitioners*. <https://www.warnathgroup.com/wp-content/uploads/2021/04/Policy-Guides-on-Protection-of-Victims-of-Trafficking-2015.pdf>

- ❖ Protasis Project. *Towards a Victim-Centered Police Response Training Manual*. https://www.eurocrime.eu/wp-content/uploads/2019/01/PROTASIS_Training-Manual.pdf

- ❖ Reddit Class Action Filing: Case Study on Platforms and Accountability. Available at: <https://www.classaction.org/media/doe-v-reddit-inc.pdf>

- ❖ Riess, H. (2017). The science of empathy. *Journal of Patient Experience*, 4(2), 74–77. <https://doi.org/10.1177/2374373517699267>

- ❖ Scanlon, M. Deep Learning Facial Image Cybercrime Investigations. PhD Thesis. Available at: <https://markscanlon.co/papers/PhDThesis-DeepLearningFacialImageCybercrimeInvestigations.pdf>

- ❖ Schneider, F., et al. "Trustworthy Cybersecurity Technologies." *Computers in Industry*, 2022. Available at: <https://www.sciencedirect.com/science/article/pii/S2666281722001287>

- ❖ Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, Council of Europe, CETS 224, 17 November 2021.

- ❖ Siegel, D., et al. Online Child Sexual Exploitation: An Emerging Challenge. Available at: <https://journals.sagepub.com/doi/full/10.1177/15570851221114396>

- ❖ Tackling Online Terrorist Content Together. Available at: https://kclpure.kcl.ac.uk/ws/portalfiles/portal/195824717/31_Tackling_Online_Terrorist_Content_Together_web.pdf
- ❖ United Nations Office on Drugs and Crime (UNODC). Global Report on Trafficking in Persons 2020.
- ❖ UNHCR. Policy on a Victim-Centred Approach in UNHCR's Response to Sexual Misconduct (UNHCR/HCP/2020/04, pp. 4 and 6). 2020.
- ❖ UNHCR. (2020). Policy on a victim-centred approach in UNHCR's response to sexual misconduct (UNHCR/HCP/2020/04, pp. 4 and 6).
- ❖ U.S. Department of Justice. Subject Matter Experts Working Group Reports. Available at: https://www.justice.gov/d9/2023-06/sme_wg_reports_combined_2.pdf
- ❖ U.S. Department of Justice. Human Trafficking and Pop-Up Brothels. Available at: <https://preventht.org/editorial/pop-up-brothels-and-airbnb-a-disturbing-human-trafficking-trend>
- ❖ Van der Watt, M. Discouraging the Demand That Fosters Sex Trafficking: Collaboration through Augmented Intelligence. 2023. Available at: https://endsexualexploitation.org/wp-content/uploads/2023_Van-der-Watt_Discouraging-the-Demand-That-Fosters-Sex-Trafficking-Collaboration-through-Augmented-Intelligence.pdf
- ❖ Verelst, A., et al. Safe Reporting Framework for Migrant Victims of Sexual Violence. Victim Support Europe, 2022. Available at: https://victim-support.eu/wp-content/files_mf/1643207415SafereportingframeworkENG.pdf

- ❖ Victim Support Europe. VOciare Synthesis Report. 2021. Available at: https://victim-support.eu/wp-content/uploads/2021/02/VOciare_Synthesis_Report.pdf
- ❖ Victim Support Europe. National Framework for Comprehensive Victim Support. 2022. Available at: https://victim-support.eu/wp-content/files_mf/1673427018NationalFrameworkforComprehensiveVictimSupportcompressed.pdf
- ❖ Victim Support Europe. (2022). National framework for comprehensive victim support. https://victim-support.eu/wp-content/files_mf/1673427018NationalFrameworkforComprehensiveVictimSupportcompressed.pdf
- ❖ Victim Support Europe. Safe Justice for Victims of Crime. 2023. Available at: https://victim-support.eu/wp-content/files_mf/1677284356SafeJusticeforVictimsofCrime_compressed1.pdf
- ❖ Victim-Centered Police Response: Communicating with Victims of Crime - A Handbook for Officers. Available at: <https://hrmi.lt/wp-content/uploads/2018/01/Handbook-for-Officers-HRMI.pdf>
- ❖ Zhu, W., et al. "Anomaly Detection in Cybersecurity Using Deep Learning Models." Electronics, 2022. Available at: <https://www.mdpi.com/2079-9292/13/9/1671>

Resources:

Digital tools:

- ❖ An extensive list of tools used for detecting of child sexual abuse can be found on the Polaris website(<https://stella-polaris.super.site/digital-tools-combating-child-sexual-abuse/detection>).

Victim-centric approaches

- ❖ Handbook for forensic child interviews in presumed cases of trafficking by Julia Korkman, HEUNI

A large version of the DISRUPT logo, identical to the one in the top right corner, centered on the page.

LOW AND INTERNET
FOUNDATION
PROMOTING THE USE OF THE
INTERNET FOR LEGAL PURPOSES



cesie
the world is only one creature



L-Università
ta' Malta



Victim Support
Europe



Co-funded by
the European Union