TRAFFICKING IN HUMAN BEINGS AND INFORMATION COMPUTER TECHNOLOGY: ITS USE BY LAW ENFORCEMENT AND MISUSE BY TRAFFICKERS IN HUMAN BEINGS

May 2024

Co-funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Co-funded and implemented by the Council of Europe
IMPETUS
Center for Internet, Development and Good Governance
EU with YOU

TRAFFICKING IN HUMAN BEINGS AND INFORMATION COMPUTER TECHNOLOGY: ITS USE BY LAW ENFORCEMENT AND MISUSE BY TRAFFICKERS IN HUMAN BEINGS

Author: IMPETUS Centre for Internet, Development and Good Management – Skopje

With contributions by
Romulus UNGUREANU and Ljupco MARKUDOV

May 2024

This publication was produced with the financial support of the European Union and the Council of Europe. Its contents are the sole responsibility of the author(s). Views expressed herein can in no way be taken to reflect the official opinion of the European Union or the Council of Europe

All other correspondence concerning this document should be addressed to the Directorate for communications, Avenue de l'Europe F-67075 Strasbourg, Cedex, France, Tel. +33 (0)3 88 41 20 00
E-mail: Horizontal.Facility@coe.int

Content

List of abbreviations

BPPOPOCC	Basic Public Prosecutor's Office for Prosecuting Organized Crime and Corruption
CA	Customs Administration
CoE	Council of Europe
EU	European Union
FP	Financial Police
GRETA	Council of Europe's (CoE) Group of Experts on Action against Trafficking in Human Beings and Trafficking in Human Beings
ICT	Information and Communication Technology
JTA	Joint Training Activities
MES	Ministry of Education and Science
MLA	Mutual Legal Assistance
MLSP	Ministry of Labour and Social Policy
MoI	Ministry of Interior
NGO	Non-governmental Organisation
NUSSMTHB	National Unit for the Suppression of Smuggling of Migrants
OSCE	Organization for Security and Cooperation in Europe
PPO	Public Prosecutor's Office
SLI	State Labour Inspectorate
THB	Trafficking in human beings
USA	United States of America

Executive summary

Council of Europe's (CoE) Group of Experts of the on Action against Trafficking in Human Beings (GRETA) prepared the Study on Online Technology-facilitated Trafficking in Human Beings (THB)[1] on the misuse of new technologies by human traffickers, as well as on the use of new technologies in detecting and identifying THB victims, collection of evidence, submission of charges against traffickers, meeting challenges and highlighting good practices from CoE member states. In order to gain a better insight into the situation in North Macedonia, the CoE Office in Skopje within the framework of the action "Strengthening anti-trafficking action in North Macedonia", which is a part of the programme framework of the European Union and the Council of Europe "Horizontal Instrument for the Western Balkans and Türkiye III", commissioned a publication on the computer information technology and trafficking in human beings.

The general purpose of this publication is to explore the current situation/ issues in detecting, investigating and prosecuting cases of THB cases committed by use and misuse of communication technology (ICT), the capacities of the competent institutions using ICT and combating ICT-facilitated crime, relevant human and technical resources as well as collection and storage of digital data.

The specific methodology applied for collecting data includes interviews and two focus groups with relevant experts and professionals working in the ICT field and combating trafficking in human beings in the field. The comments/ recommendations from the round table with representatives of state institutions and the civil society sector were subsequently incorporated into the document.

The main findings and results define the problems and issues faced by the competent bodies, inform about the capacities of the competent institutions, of available resources, on ways of handling of digital data and offer recommendations and resources for enhanced prevention and fight against ICT-facilitated THB.

[1] GRETA, Online and technology-facilitated trafficking in human beings, Full report, April 2022, https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49

ICT gives criminals an opportunity to increase the "THB market" and reduces their risk of being caught by the law enforcement agencies. Since the risks and criminal liability are low, the ICT-facilitated THB is attractive to traffickers in human beings. In addition, the users of these illicit services can enjoy them without any consequences. Traffickers have learned to abuse technology so as to develop and deliver new contactless services, such as cybersex trafficking. In fact, technology is used to create a global marketplace where customers in one part of the world can pay for the services provided by THB victims who are exploited in another part of the world. Technology allows traffickers to increase the amount of information in the marketplace, and thus, providing access to a wider easily accessible offer to "its clients", leading to an overall increase in transactions.

In the Republic of North Macedonia, the National Unit for the Suppression of Smuggling of Migrants and Trafficking in Human Beings (NUSSMTHB) was established within the Ministry of Interior (MOI), resulting in an increase of THB investigations in the past years. However, in order to improve anti-trafficking efforts and provide assistance to potential victims, it is necessary to establish accessible tools and online reporting channels. For this purpose, it is necessary to promote and increase the visibility of the MOI online tool "Red Button" and introduce a hot line exclusively dedicated for reporting THB cases in order to enable citizens to report cases anonymously, and if necessary, use a possibility to locate the THB victim through the mobile operators. These two components are the key to facilitating reporting, intervention and assistance in THB cases.

As for the legal aspects, there is a need for a though review of the current legislation and its available tools on proactive detection of criminals who have committed the crime of online stalking and sexual harassment. The law does not allow secret (covert) online investigations (secret infiltrations). It is also necessary to sensitize and inform the law enforcement agencies, and the judicial authorities (the MoI, the inspection authorities, the public prosecutor's office and the courts) about good practices, which can be applied in the preventing and combating ICT-facilitated THB cases.

The assessment of the various institutions involved in the criminal justice chain and the inspection revealed substantial issues related to human resources. There are two critical aspects: inadequate staffing levels and difficulties in effectively managing these resources. Additionally, a lack of appropriate data collection software and a digital inter-institutional connectivity make their collaboration and investigation difficult. Mobile teams annually identify a significant number of potential THB victims,

but are not connected in an electronic database with other relevant institutions (PPO, MoI, courts, SLI). Local police and certain border officials do not conduct thorough investigations in accordance with THB indicators, therefore unidentified trafficked persons were sometimes deported without being referred to the appropriate authorities. The authorities thus missed to obtain meaningful information about the ways in which THB crimes were committed.

The National Reporter on Trafficking in Human Beings in the Office of the Ombudsman recommends improving identification of victims through analysis and monitoring of new *modus operandi* for THB such as by misuse of the Internet, of the new communication and information technologies, and by preparation of appropriate indicators for the purpose of recognition, monitoring and timely detection of THB victims.

The law enforcement agencies and labour inspectorate face many limitations in their ability to proactively investigate THB crimes. These challenges stem from insufficient human, financial and technical resources, as well as a lack of access to modern technical tools needed to effectively conduct proactive investigations. In order to effectively investigate cases of ICT-facilitated trafficking in human beings, investigators must possess appropriate technical expertise and skills.

Regarding digital evidence, while it is difficult to store and keep them, it is important to insist on drawing up clear written rules and procedures for dealing with electronic evidence that the police should be trained on. The police should be provided with appropriate technical equipment for handling and storing electronic evidence. An additional in-depth assessment by technical experts and expert analyses of the existing technical resources of the law enforcement agencies is needed, in order to assess the need for upgrading the capacities for detection and investigation of ICT-facilitated THB.

Raising public awareness among citizens about the seriousness of the online THB, as a preventive measure, is a multifaceted endeavour that includes consistent awareness raising campaigns and comprehensive media coverage. An essential aspect of this effort includes the development and dissemination of promotional materials that are specifically tailored for students, teachers, and parents. The materials have a dual purpose: to raise awareness about the dangers lurking online and to impart strategies on self-protection and protection of the loved ones from the digital dangers.

This publication offers practical recommendations, prepared according to the GRETA study, and adapted to the context of North Macedonia. Its objective is to share information and knowledge, and use it for trainings targeting the law enforcement, the prosecution, the judiciary, lawyers and civil society organizations. The specific aim is to strengthen knowledge about the ICT-facilitated THB investigations, understand the challenges and enhance the capacity to effectively deal with them by raising awareness of the competent authorities about the latest trends in the work methods and investigative tools that are accessible with the help of ICT.

Recommendations related to the detection of the ICT-facilitated THB, the operational aspects in terms of investigation and prosecution, securing digital evidence and prevention by way of raising public awareness should be used for future activities that contribute towards sustainable capacity building activities, knowledge transfer and strengthened expertise of the key stakeholders (the law enforcement, the judiciary, lawyers, inspectors, civil society organizations, the media, social workers, etc.).

1. Introduction

New technologies allow traffickers to recruit and exploit victims, while simultaneously creating opportunities for the law enforcement agencies to apply them to prevent and fight these crimes. In April 2022, the Council of Europe's (CoE) Group of Experts of the on Action against Trafficking in Human Beings (GRETA)[2] published a Study on Online Technology-facilitated Trafficking in Human Beings[3] on the misuse of new technologies by human traffickers, as well as on the use of new technologies in detecting and identifying THB victims, securing evidence and charges against traffickers, on the challenges and good practices from the CoE member states. The Study has a wide scope. It gives an assessment of the extent to which technology affects trafficking in human beings, as well as insight into the manner in which the traffickers operate in the context of ICT-facilitated THB. Its focus is on exploring operational and legal challenges faced by member states – and to some extent NGOs – in detecting, investigating and prosecuting online ICT-facilitated trafficking in human beings, as well as in identifying victims and raising awareness among risk groups. Moreover, the Study explores strategies, tools and good practices adopted by the member states and NGOs for overcoming the existing challenges and improving the response to the ICT-facilitated THB. It reveals similarities between the countries and depicts country-specific experiences. Particular focus is placed on trainings – bearing in mind that investments in human resources are as important as the investments in technological tools. The recommendations drawn in the Study refer to activities to improve detection, investigation and prosecution of ICT-facilitated THB cases; to enhance cooperation with private companies and international cooperation; to provide capacity-building activities; to review legislation and to prevent victimisation and re-victimisation. The Study was conducted as part of the CoE's long-standing interest in the issue

[2] https://www.coe.int/en/web/anti-human-trafficking/greta The Group of Experts on Action against Trafficking in Human Beings (GRETA) is an independent body monitoring the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings. All member states of the Council of Europe are obliged to respect the Convention, as well as the non-member states, Belarus and Israel.

[3] GRETA, Online and technology-facilitated trafficking in human beings, Full report, April 2022, https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49

of technology and fight against THB. In addition to offering a *systematic assessment of the current evidence data base*, this Study also seeks to provide a tool for conducting future assessments and monitoring changes in the technological and behavioural states of GRETA and other entities.

In order to gain a better insight into the situation of North Macedonia, the CoE Office in Skopje as part of the action "Strengthening the anti-trafficking action in North Macedonia", within the programmatic framework of the "Horizontal Instrument for the Western Balkans and Türkiye III" of the European Union and the Council of Europe, commissioned this publication.

The overall aim is to explore the current situation/issues in detecting, investigating and prosecuting cases of the ICT-facilitated THB, of the competent institutions using ICT and combating ICT-facilitated crime, of the country's human and technical resources and of handling digital data.

The specific objectives are:

- to present the latest developments in THB cases (conducting investigations, inter and intra-institutional cooperation and communication, the use of technologies, challenges in information exchange and international cooperation) and the *modus operandi* of the perpetrators (including criminal networks),
- to present, analyse and evaluate ICT-facilitated investigation methods, tools and techniques for gathering, securing and using electronic evidence in THB cases,
- to outline challenges, issues with evidence (in particular the securing, protection, proper handling and processing of electronic evidence), lessons learnt, best practices for investigating ICT-facilitated THB and to explore ways for improving operational cooperation.

Similar to the GRETA Study, ICT is defined as "information and communication technologies, specifically those consisting of digital and network environments. Technologies that enable users to exchange digital data across networks including the Internet, online social networks, and mobile phones"[4].

This publication contains concrete recommendations, developed according to the GRETA Study, but adapted to the context in North Macedonia. Information contained herein is to be widely disseminated and used for the capacity-building activities planned as part of the CoE action, targeting the law enforcement, PPO, the judiciary, lawyers and civil society organizations.

[4] Latonero, M., The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking. University of Southern California, Annenberg Centre on Communication Leadership & Policy, 2012

The aim is to strengthen knowledge about the key challenges in ICT-enabled THB investigations and to increase the state capacity to effectively deal with them by offering concrete recommendations and raising awareness of the competent authorities about the latest trends in the investigative methods and tools.

2. Methodology

2.1. Interview

Semi-structured interviews were conducted with three target groups:

1. The first target group included representatives of state institutions, experts, judges and public prosecutors, lawyers and members of academia for collecting information regarding the work of state institutions in charge of detecting, investigating and proving cases of ICT-facilitated THB.
2. The second target group included representatives from civil society organizations in order to perceive and compare their experiences and their findings from conducted research and/or direct work (support/assistance) with THB victims. Civil society organizations that were invited to participate in the interview are the members of the Secretariat and the Subgroup for Combating Child Trafficking of the National Commission for Combating Trafficking in Human Beings and Illegal Migration, as well as local civil society organizations that work in this field.
3. The third target group included representatives from technology companies, internet providers, telecommunications companies, ICT companies from North Macedonia, etc.

The interviews were used to scan the situation with respect to the state institutions (competencies, operational procedures for investigation, capacities, relations and cooperation) and the support that civil society organications can offer in detecting victims and perpetrators.

The interview questions were open-ended, so respondents were asked to provide feedback and elaborate their responses regarding a specific procedure, issue, and challenge from their work domain. We used the same questionnaires from the GRETA Study. Questionnaires for the three target groups are attached as an annex to this publication.

2.2. Focus groups

Separate discussions were held in two focus groups. The focus groups were held in a hybrid format (in the CoE office and online via Zoom), lasting an hour and a half each.

The purpose of the first focus group was to discuss the activities carried out by the civil society organizations at the local level and their capacities, as well as the evaluation of the local responses and capacities of the law enforcement agencies at the local level in relation to the novelties in ICT-facilitated trafficking in human beings. At the same time, together with the participants, we made an effort to find out about practical issues and challenges in the inter-institutional coordination and cooperation at the local level. Participants in the discussion in this focus group were representatives providing legal aid and assistance to victims, and representatives from local prevention councils.

The purpose of the second focus group was to analyse national policies and strategies and state responses regarding the novelties of the ICT-facilitated THB and to reveal gaps, inconsistencies and challenges in the legislation and capacities for the inter-institutional coordination and cooperation. Participants in the discussion in this focus group were representatives from the Secretariat of the National Commission for Combating Trafficking in Human Beings and Illegal Migration, as well as representatives from the judiciary.

Ljupcho Markudov, expert on trafficking in human beings and illegal migration, Jasmina Dimitrieva, Senior Project Manager and Aleksandar Efremov, Project Assistant from the Programme Office of the Council of Europe in Skopje participated as observers in the two focus groups.

The questions discussed in the two focus groups are given in the Annex.

2.3. Round table

After the interviews and focus groups were completed and the requested data collected, analysed and summarised in a draft report, the preliminary findings with conclusions and recommendations were presented and elaborated in a round table with 23 representatives of the institutions in North Macedonia, in charge of investigation, criminal prosecution, and adjudication of THB crimes, the non-governmental sector and international organizations. The findings of the discussions have been used to refine and finalise the report, its conclusions and recommendations. The participants had the opportunity to confront their opinions and perceptions and jointly derive relevant guidelines and advice for improving the capacities and procedures used by all stakeholders involved in dealing with ICT-facilitated THB.

3. Current situation

The legal framework for combating trafficking in human beings in the Republic of North Macedonia[5] is solid and there is a continuous progress and appropriate changes according to the recommendations of the relevant international organisations. Thus, in its third evaluation report[6] published on 24.03.2023, GRETA welcomed the progress of North Macedonia in the development of the legislative framework for combating trafficking in human beings. However, certain recommendations were given for improving the legal framework, especially in the area of providing assistance to THB victims. The establishment of the National Unit for the Suppression of Smuggling of Migrants and Trafficking in Human Beings (NUSSMTHB) and the increase in the number of convictions compared to the previous assessment period were also welcomed. However, the authorities were requested to clarify the mandate of the State Labor Inspectorate and provide it with adequate human and financial resources, as well as strengthen human, financial and technical capacities of the law enforcement agencies so as to enable them to proactively investigate THB cases, collect and use all possible evidence, including evidence gathered through special investigative measures, and financial and digital evidence.

North Macedonia participates in the Network of the National Coordinators for Combating Trafficking in Human Beings of Southeast Europe. In 2018, it adopted a Joint Declaration of the Ministers Regional Cooperation to combat

[5] The legal framework consists of the following legal regulations: Criminal Code, Law on Foreigners, Law on State Compensation for Victims of Violent Crimes, 2017-2020 National Strategy and Action Plan for Combating Human Trafficking and Illegal Migration, 2021-2025 National Strategy and Action Plan for Combating Trafficking in Human Beings and Illegal Migration, 2021-2025 Action Plan for Combating Trafficking in Children including the Operational Plan for Combating Trafficking in Children, Standard Operating Procedures for Dealing with Victims of Trafficking in Human Beings, Standard operating procedures for dealing with vulnerable categories of foreign persons, Standard operating procedures for dealing with unaccompanied foreign children, Indicators for identification of victims of human trafficking, Indicators for identifying presumed and potential victims of human trafficking in cases of mixed migration movements , Indicators for identification of child and young potential THB victims for the purpose of labour exploitation.

[6] GRETA, Evaluation Report, North Macedonia, Third evaluation round: Access to justice and effective remedies for victims of trafficking in human beings, 24 March 2023, https://mk.usembassy.gov/2021-trafficking-in-pershttps://lastrada.org.mk/kampanji/2846-2/?lang=en

Trafficking in Human Beings[7]. The Declaration re-affirms the commitment for the protection of victims, prosecution of perpetrators, prevention of trafficking in human beings, as well as for the establishment of compensation schemes for victims. It recognises the importance of reducing the demand for services from THB victims and emphasises the relevance of the ICT in combating trafficking in human beings.

The 2022 US Trafficking in Persons Report[8] notes that the authorities have made significant efforts to achieve standards for eliminating trafficking in human beings. These efforts include prosecuting multiple defendants and applying the victim-centred approaches to reduce re-traumatisation of the child victims. According to the Report, the authorities identified significantly more victims and showed an overall increased effort in the prevention and in collecting feedback from THB survivors. However, authorities have convicted fewer traffickers and the police remains under-resourced and under-equipped to conduct proactive investigations. Similarly, the Basic Public Prosecutor's Office for the Prosecution of Organized Crime and Corruption (BPPOPOCC) lacks sufficient human resources, and a digital case management system to deal with the cases under its jurisdiction. Although mobile teams, which identify the largest number of potential victims every year, have been re-activated, sufficient funds have not been allocated to them, despite promises. Local police and some border officials did not consistently apply THB indicators, and have deported persons who could be THB victims, without referring them to the appropriate services or protection measures to prevent their re-victimisation.

The Ombudsman - National Rapporteur on trafficking in human beings and illegal migration is tasked with monitoring and evaluating the overall situation and activities for combating trafficking in human beings and illegal migration, with collecting and analysing data from relevant institutions and organizations, with monitoring and evaluating the implementation of the National Strategy and Action Plan for combatting trafficking in human beings and illegal migration. The National Rapporteur has issued recommendations for improving the efficiency and effectiveness of the fight against trafficking in human beings and illegal migration, for improved institutional response and for a revision of the strategic goals. Since this position was established in 01.12.2019, three reports have been issued that focus on different stages of the THB process[9]. The reports do not focus on the effectiveness of the

7 Joint Declaration of the Ministers of Interior of South-East Europe on Regional Cooperation in SEE to combat Trafficking in Human Beings, 16 March 2018

8 2022 US Trafficking in Persons Report, TIP Report 2022 - U.S. Embassy in North Macedonia (usembassy.gov)

9 The 2020 Report on the challenges in the identification process of victims of trafficking in human beings; The 2021 Report on the challenges and efficiency of the competent

investigative authorities in dealing with the ICT-facilitated THB. Only the 2022 report gives a recommendation to improve the identification of victims through investigation and monitoring of new *modus operandi* for trafficking in human beings involving the internet, by use of new communication and information technologies, as well as by development of appropriate indicators for timely detection and identification of THB victims.

In 2023, the crimes of stalking and sexual harassment were included in the Criminal Code[10]. They prescribe a fine or imprisonment of up to three years for the perpetrator who stalks, that is: "*...follows, pursues, or otherwise interferes with the private life of another person without any authorization or establishes or tries to establish unwanted contact with them by coming in the space where that person resides, by misuse of personal data, by using means of public information or other means of communication, or psychologically abuses, harasses or intimidates the person in any other way and thereby causes a feeling of insecurity, anxiety or fear for his or her safety or the safety of their beloved*". The penalty is stricter, if this crime is committed by a person close to the victim, that is, a current or former intimate partner. If a child is a victim of this crime, the maximum penalty is up to five years terms of imprisonment. This was the legislator's response to the case that came to light in 2020 – the so called "Public Room case", where photos and videos of girls (some sent in confidence, others taken from social networks and photoshopped) were shared in a closed group on the Telegram application, with inappropriate comments and with contacts from the victims. There were also minors among the victims. The above amendment also incriminated sexual harassment: *"... those who by verbal, non-verbal or physical action, as well as by use of electronic means of communication with explicit or implicit, real or symbolic meaning, by indecent offer, luring, expression of sexual passion or by any other action that clearly resembles sexual intercourse or other similar sexual acts, which harms dignity of another, provokes discomfort, annoyance, humiliation, or fear shall be punished with an imprisonment of up to one year*". If the crime is committed against a subordinate or a dependent person, a colleague or in a public place or against a person who is vulnerable due to his or her age, illness, disability, drug addiction, pregnancy or severe physical or mental disorders, the prescribed sentence is higher and ranges from six months to three years imprisonment.

institutions in the Republic of North Macedonia in the process of prevention, identification and implementation of the protection of victims of trafficking in human beings; The 2022 Report on the challenges in the identification and reintegration as conditions for supporting victims of human trafficking in the Republic of North Macedonia.

[10] Law on Amendments and Supplements to the Criminal Code, Official Gazette of the Republic of North Macedonia no. 36/2023 dated 17.02.2023.

4. Practical challenges in detecting ICT-facilitated trafficking in human beings

This section presents the ways of detecting and reporting trafficking in human beings in North Macedonia, the impact of ICT on the commission of this crime, as well as the challenges associated with investigating and prosecuting ICT-facilitated THB. Regarding the technology-facilitated detection, investigation and prosecution of trafficking in human beings, the GRETA Study identified the following challenges, which will be compared and discussed in the context of North Macedonia:

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

4.1. How to identify and report

Often, THB victims do not report the crime, because they do not recognise the case and its seriousness, that is, they are not even aware that they were victims. In the few cases in which they report, they do not understand that they are THB victims, but report because they feel tricked, deceived or disadvantaged, especially when it comes to labour exploitation. The situation is similar when the THB victims are children, especially in the cases of ICT-facilitated recruitment. Children do not report and tend to hide the cases from their parents out of shame. But when they can no longer bear and "control" the situation they are in (realistically, they never were in control, the predator was the one in control), only then do they talk to their parents/guardians and confide in them about what had happened to them. However, even in such situations, there are cases where parents/guardians do not report to the authorities in order to "avoid embarrassing" the family.

Reporting cases of trafficking in human beings to the police is possible through the online tool Red Button (Црвено копче)[11] available on the website of the Ministry of the Interior, which can be used by the victims, but also by any citizen who has any knowledge or information about child abuse, hate crime and incitement to violence, as well as trafficking in human beings. However, for cases that are urgent, or for which there is evidence that they being committed at the moment, instead of reporting on the available application, citizens should immediately report the cases on the 192 phone number. There are no indicators to measure the effectiveness of this tool. This could be done, for example, by analysing the reported cases' statistics through this application and data related to these cases' final conclusion. In this regard, the 2021 US Trafficking in Persons Report[12] states that "*The Government of the Republic of North Macedonia did not operate a hotline for reporting irregularities, but the MoI has an application to report various crimes, including trafficking in persons; the application received three trafficking-related reports in 2020*".

The MoI has also opened an email address cybercrime@moi.gov.mk for reporting any form of cyber/online crime.

The following civil society organizations provide opportunities for reporting, informing, and supporting THB victims:

[11] https://redbutton.mvr.gov.mk/default

[12] 2021 US Trafficking in Persons Report, Trafficking in Persons Report 2021 - U.S. Embassy in North Macedonia (usembassy.gov)

- Open Gate - La Strada operates the SOS line for information, support and protection against trafficking in human beings - 0800 11111,
- The First Children's Embassy in the World – Megjashi operates the SOS telephone number for children and youth: 0800 1 2222 (toll-free line),
- The Macedonian Association of Young Lawyers and the SOS Children's Village (SOS Detsko Selo) offer legal support to vulnerable victims of violent crimes - legal support: 075238837 and psychological support: 071277180,
- The Women's Organization of the Municipality of Sveti Nikole has an office for free legal assistance, and psychological and social support: it offers phone consultations with a psychologist, at 032444620 or via email at womsvetinikole@yahoo.com.

Respondents in this survey indicated that there is no easily accessible and visible system for reporting content and websites suspected of being related to illegal activities, including trafficking in human beings for sexual and labour exploitation in North Macedonia. If there is such a system, for example, on the websites of the law enforcement agencies, it would be possible for any person to report suspicious websites, content, profiles, etc., and the relevant institutions could react in a timely manner.

THB cases are reported to the local police station with territorial jurisdiction, the basic public prosecutor's office and the centre for social work. According to the information gathered from the interviews with the respondents in the research, the existing protocols for inter-institutional coordination in the field and the operational procedures are not fully respected by the local entities, so the opening and management of the cases goes slow. The civil society organisations that provide legal, psychological and social assistance to THB victims and act against cyber violence complain about a lack of communication with the law enforcement agencies. They believe that they can share information relevant for the investigation, which they obtained through the communication with the victims. There were also cases when the civil society organizations reported cases of fraud (fraudulent online job vacancies), but were told that "now was not the time" to deal with them. So, the civil society organisations expressed doubts about the competence and professional work of the authorities competent to deal with these cases. The reasons for the inadequate case processing may be found in the insufficient expertise and skill for documenting the case and securing evidence, as well as in the absence of software tools for proactive online identification of fraudsters by the competent authorities at the local level.

Considering that the local police officers do not have enough knowledge about trafficking in human beings and do not regularly notify the NUSSMTHB at the Ministry of the Interior about the existence of potential cases, the identification of THB victims is lacking.

Several court proceedings for trafficking in human beings have been ongoing for a period of more than 5 years, and given this time period, gathering evidence has been extremely difficult.

4.2. The impact of ICT on trafficking in human beings

The corona crisis worsened the problem of child trafficking, 16.08.2021
https://novamakedonija.com.mk/makedonija/politika/корона-кризата-го-продлабочи-проблем/

Lejla Dervišagić, Head of Operations of the Council of Europe Programme Office in Skopje:
The Internet and social networks play an important role in child trafficking. Social networks are the most used for information sharing and dating of young people, but they also bring great danger to them, so it is of great importance to design and adopt preventive and protective measures. If in the past children did not have access to mobile phones, computers and the internet, today the youngsters make daily use of them. Access to these technologies increases the occurrence of "seduction", that is, grooming, through video game sites and social networks. Reports indicate that during the COVID-19 pandemic, online recruitment and exploitation of children through social networks had significantly increased.

During and after the crisis caused by the COVID-19 pandemic, people transferred a large part of their work activities, interaction, communication, and even their way of life to the online space and increasingly use ICT. The volume of online activities is continuously increasing. Criminals, including human traffickers, have also adapted to such trends. Human trafficking as a crime is increasingly being committed over the Internet, and the fact that the age limit is decreasing is also worrying. If ten years ago, the victims were 16 years old and up, now they are between 10 and 17 years old. Criminals are increasingly targeting groups that use the internet the most, and are the least informed about its dangers. So, finding and recruiting victims for

sexual and labour exploitation, including children, is conducted through new forms of communication - social media, platforms, forums. The use of online communication allows greater anonymity and a greater profit for the criminals, and thus, they increasingly focus on recruiting and controlling victims through internet communication. The traffickers first establish communication, that is, get to know the impersonating victims through fake profiles to gain their trust, get to know their family circumstances, identify their weaknesses and desires, go on live dates, and then proceed to use blackmail and fraud in a variety of ways. Mostly these are cases of sexual exploitation, but victims are also recruited for marriages and for labour exploitation. Finding clients interested in using the services of the exploited persons also takes place online.

Serbian police arrested 12 paedophiles who were stalking victims from 7 to 14 years of age on the Internet, 20.09.2023
https://mia.mk//story/акција-на-српската-полиција-уапсени-12-педофили-кои-на-интернет-демнеле-жртви-од-7-до-14-години

In the "Armageddon" police operation, throughout Serbia, a group of 12 paedophiles were arrested on a suspicion of having committed the crimes of displaying, obtaining and possessing pornographic material and exploiting a minor for pornography and sexual harassment.
They are suspected of using file sharing applications, downloading, storing on hard drives and sharing content created by exploiting children for pornographic purposes via the Internet, over a long period of time, and also for entering into communication from their accounts with minors, sending photos and videos of pornographic content and collecting content resulting from the exploitation of minors through social networks.
During the search of the suspects' apartments and the inspection of the computers, the police found a large amount of video clips and photos created by using minors for pornographic purposes, content for sexual exploitation of children aged 7 to 14 and other photos and videos of explicit child abuse for pornographic purposes, as well as messages with sexual content the suspects sexually harassed children and minors with.
The operation "Armageddon" was launched in 2010 and hundreds of people have been arrested todate. In Serbia there are 675 registered paedophiles.

Criminals, or predators as they are called, since they stalk, identify and then attack, use cyberspace to recruit THB victims for several reasons:

- **Anonymity**: the internet allows them to hide their true identity by creating and using fake profiles on social media and other platforms, making it difficult for law enforcement to track and detect them. It is the anonymity that provides a sense of security for predators.
- **Access to a wider audience**: the internet provides access to a huge and diverse target group of potential victims. Predators can target individuals from different locations and backgrounds, which increases their chances of finding vulnerable targets.
- **Easy communication**: online platforms provide easy and private means/channels of communication. Predators can find and connect with potential victims through messaging apps, social media, email, chat rooms, certain online games, making it easier to build trust and manipulate them over time.
- **Opportunities to establish trust**: predators use the online space to establish contact and gain the trust of victims, to understand their vulnerabilities and to gradually manipulate them into exploitative situations.
- **Global reach**: trafficking in human beings is often transnational and sometimes involves transporting victims across borders. The Internet allows traffickers to coordinate and manage such operations regionally and globally, from recruitment to transportation and exploitation, without the victims ever leaving their house.
- **Reduced physical risk**: unlike recruitment that used to take place in person, which can be risky for traffickers due to potential public exposure and easier detection by law enforcement agencies, the online recruitment minimises the physical risks associated with trafficking activities.
- **Low costs**: online recruitment can be cost-effective for traffickers compared to traditional recruitment methods. They can reach out to more potential victims without significant costs.
- **Impersonal approach**: some predators may more easily blackmail their victims when communicating online, which facilitates psychological control and dominance over them.
- **Availability 24/7**: the internet is on all the time, allowing predators to contact and mingle with potential victims online at any time in the day or night, and thus increasing their chances of successful recruitment.

The rise of the artificial intelligence (AI) is creating an additional problem. Although its use in the commission of trafficking in human beings is not widespread, it is still a worrying trend. Some of the ways in which traffickers could use AI include, for example, using AI-driven algorithms for recruitment and advertising purposes, using manipulated (altered) images and videos to create fake profiles or generate explicit content, as well as to reach out to a larger online market through the use of AI-driven platforms or applications. Moreover, the cryptocurrencies, that is, the online payment systems used by traffickers and their clients that allow them anonymity and fast payment, make it more difficult for the law enforcement to track financial transactions and detect traffickers. The cryptocurrencies are used, because they enable unobstructed payment across borders, bypassing restrictions on cash transfers between countries. The use of multiple digital "wallets" (a separate wallet for each transaction) creates additional challenges for the police and the anti-money laundering authorities to track transactions and trace patterns.

Human trafficking: Criminals target children who use the internet the most, and are the least informed about the dangers lurking online, 18.10.2022
https://www.slobodenpecat.mk/trgovija-so-lugje-kriminalcite-gi-targetiraat-decata-tie-najmnogu-go-koristat-internetot-a-najmalku-se-informirani-za-opasnostite-koi-gi-demnat-onlajn/

According to the National Coordinator for Combating Trafficking in Human Beings and State Secretary in the Ministry of the Interior, Magdalena Nestorovska, online communications, as much as they have positive effects to informing the citizens, they also have negative effects resulting from insufficient awareness about the misuse of the online communication.
Human traffickers carry out many of their preparatory criminal activities and even commit the THB crime by misusing the computer technology. This means that they have managed to recruit the victim because, he or she is not sufficiently aware about the extent of misuse of the computer technology, but also for the criminals committing the criminal act, ICT enables greater anonymity and greater profits, emphasises Nestorovska. She adds that there are a total of 8 THB victims in the current year, of which 7 are minors. She adds that one of these 8 people was an identified THB victim through online communication.
This means that the criminals target the group that uses the internet the most, but it is the least informed about the dangers coming from the abuse of the information technology, says Nestorovska.

According to the information from the legal practitioners participating in the interviews and focus groups, recently, the law enforcement agencies have observed an increasing number of cases of trafficking in human beings where ICT was misused (for recruiting victims, exploiting, etc.). It should be noted that ICT has been also misused in THB cases previously, but in the recent period, after the COVID-19 pandemic, the internet has been used more frequently. Most often, the communication between the trafficker and the victims started and took place through social networks, such as Instagram, Facebook, Messenger, etc. The victims are young, not even 20 years old.

In addition, in the eastern part of the country, there have been many arranged marriages, which is already part of the tradition of certain local communities. In most of the cases, newlyweds are minors, and their parents decide for the marriage. Most of the cases are not reported and processed by the law enforcement agencies. In 2022, 6 minors were identified as victims of forced marriage[13].

Along those lines, the Third Evaluation Report of GRETA[14] notes that the number of formally identified THB victims is low (between 2 and 9 per year, except in 2021 when 48 THB victims were identified, 39 of were from Taiwan) with a shift towards labour exploitation as the dominant form of exploitation. In the case of the people from Taiwan who came to North Macedonia[15] ICT was used to recruit them, but also for defrauding committed by the victims under the threat of traffickers. The victims had to establish contacts with potential victims of financial fraud through internet. They were divided into three groups as telephone operators working at three levels. The "operators" in the first level presented themselves as officials in a bank, postal service or insurance company to the victims. In the second level, in order to obtain a complete personal data, the victims pretended to be police officers and demanded a proof from the victims about the payment of a fictitious fine, and managed to steal personal data of the victims. The third-level "operators", pretending to be prosecutors and judges, convinced the victims that they

[13] Радио Слободна Европа, Тренчевска: Годинава три девојчиња биле цел на сексуална експлоатација, 30.05.2023 [Radio Free Europe, Trenčevska: This year three girls were the target of sexual exploitation, 30.05.2023], https://www.slobodnaevropa.mk/a/32435138.html

[14] GRETA, Evaluation Report, North Macedonia, Third evaluation round: Access to justice and effective remedies for victims of trafficking in human beings, 24 March 2023, https://rm.coe.int/greta-evaluation-report-on-north-macedonia-third-evaluation-round/1680aaa573

[15] Пресечен меѓународен канал за трговија со луѓе од Тајван, 28.05.2021 [International Human Trafficking Channel for people from Taiwan Intercepted, 28.052021], Пресечен меѓународен канал за трговија со луѓе од Тајван – ЈАВНО ОБВИНИТЕЛСТВО НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА (jorm.gov.mk)

would face heavy charges, unless they cooperate and transfer a certain amount of money to certain accounts in order to obtain a smaller fine, or not pay a fine at all.

According to the respondents of the research, there are also agencies in the country for a temporary employment that are offering opportunities for "work and travel" for students. These agencies are not licensed to provide such services and their operations are not checked. The most common target are the students. Recently, Greece and Turkey have been offered as work destinations, especially in the agricultural sector. Several students complained that the working conditions were not what they have been promised and agreed upon at the beginning, and that even their freedom of movement was limited.

Labour exploitation is the second most prevalent form of trafficking in human beings in the entire Balkans and most often occurs in the agricultural, industrial, textile and hospitality sectors. Traffickers can also use the internet to recruit victims of labour exploitation. The fake job platform "Work in EU", which the NGO "Open Gate" used to raise awareness among job seekers, indicated that a large number of users of this platform were not at all aware of the risk posed by the fake job advertisements abroad.[16]

Online predators are a major threat to children. They use the internet and ICT tools to recruit THB victims and exploit them. Children are most often the victims, as they carelessly share their data, pictures and videos with other people. This type of exploitation usually begins with some kind of psychological manipulation (establishing a relationship with the minor victim), then "sexting" (creating and/or sharing sexually suggestive images of the victim), "online" sexual blackmail (blackmailing the child victim with the above images, so as to extort sexual favours or money) or live sexual abuse (forcing a child into sexual activities) and distributing sexualised material depicting children.[17]

In one school, several girls had a problem with the same predator. The local police also responded, but the reporting procedure of the MoI was not followed, so the problem remained to be resolved within the school, without initiating an appropriate criminal law procedure.

---

[16] La Strada – Open Gate, Opportunity or Exploitation, https://lastrada.org.mk/kampanji/2846-2/?lang=en

[17] ECPAT International, Online child sexual exploitation: A common understanding, 2017, https://www.ecpat.org/wp-content/uploads/2017/05/SECO-Booklet_ebook-1.pdf

Children victims of the pandemic: Smuggling of migrants and trafficking in human beings are the growing trends, minors mostly trafficked for sexual exploitation, 20.08.2021
https://denesen.mk/decata-zrtvi-na-pandemijata-raste-kriumcharenjeto-i-trgovijata-so-lugje-maloletnite-najchesto-za-seksualna-eksploatacija/

Ljupcho Markudov, Head of the Unit for Trafficking in Human Beings and Smuggling of Migrants and Assistant Head of the National Unit for Suppression of Smuggling of Migrants and Trafficking in Human Beings, described one of the ways to recruit THB victims through internet:

A 15-year-old girl from a broken family, divorced parents, the mother is not interested in the child, the father lives abroad. The girl gets in touch with a boy, two to three years older than her, through a social network, they get closer, they arrange dates. She meets the boy twice, and in the third meeting the boy's "father" appears. They are taken to another city in our country, they live together in an apartment, they go to coffeeshops, tourist places, the girl is happy, she finally finds something that feels like love, but the situation changes very quickly. The girl is locked in an apartment in one of the towns in the country and under the influence of drugs and alcohol, she is brought into a state of obedience and forced to provide sexual services to men.

Many children, although they are not ready for marriage, neither physically nor mentally, are forced into marriage and are sexually exploited by the whole family, forced to do hard physical domestic work that does not correspond to their age, mental and physical development. Very often they also do heavy field work or begging, market work, etc. These are the main forms of exploitation when it comes to children.

For the schools, there is the 2021 Protocol for Violence Prevention and Response, which also addresses sexual and cyber violence[18] as types of

[18] The protocol defines sexual violence as "sexual act committed or attempted against a victim who did not freely give consent, was or is unable to consent and refused unwelcomed sexual advances, requests for sexual Favors, and other verbal, nonverbal, or physical conduct of a sexual nature Sexual violence includes: inciting and coercing someone into performing sex acts, abusing the person and creating an unsafe space, using and distributing audio and visual materials". Furthermore, cyber violence is defined as "a type of harassment and direct acts of violence through the use of ICT tools and technologies such as mobile phones, computers and the internet. All actions such as

violence which students can be subjected to. The protocol aims to inform and educate all stakeholders in the schools (students, parents, teachers, etc.) about how to report, act and react in case of violence. All stakeholders should be well aware of this Protocol and encouraged to report any signs or cases of online abuse of children.

Teenagers can join online social networks, but it is still mandatory to check on them regularly, in order to protect their safety and privacy. Parents and guardians are crucial in protecting children online and must be more vigilant and control how their children use the internet. It is possible to set a limit on the time spent on the internet by the child in the course of a day. In addition to parents, teachers should also be concerned about the online safety of the children and young people and should remind students about the safe use of the internet and the potential dangers lurking in the online space.

Cyber violence also includes *sexting*.[19] It refers to sending, or receiving sexually explicit content, such as pictures, videos or text messages, usually via mobile phones. This practice covers a range of activities, such as: sharing sexual or explicit images, exchanging nude photos and selfies, sending sexually suggestive text messages, sharing images in underwear or with minimal clothing, etc. Young people feel that sharing intimate images with only their boyfriend or girlfriend is acceptable. However, creating or distributing sexual images or videos involving children below the age of 18 is actually illegal. Forwarding such explicit content, actually constitutes production and distribution of pornographic material to minors, which is defined as a crime in the legislation. *Sexting* and forwarding have many consequences. Once a photo or image is sent to someone, the control over its further distribution is already lost. Even when it is sent to someone who can be trusted, anyone can transmit this content to third parties, or store it online. If this happens and the content becomes public, the psychological consequences for the victim have already occurred (shame, humiliation, remorse, regret, mistrust, self-isolation, depression, anger, hatred, aggression, etc.).

An important channel that carries various threats to children, ranging from privacy breach and abuse, to manipulation and radicalisation, are the

exchanging photos and videos, sending messages (e-mail, SMS, chat), direct/indirect exchanging and publishing information of a sensitive nature about a person, creating fake profiles and other actions without prior direct consent, inciting and performing violence through social networks are counted as elements of cyber violence".

[19] More information about sexting at the following links: https://www.britannica.com/topic/sexting, https://www.plannedparenthood.org/learn/teens/bullying-safety-privacy/all-about-sexting, https://www.verywellfamily.com/what-is-sexting-problem-1258921, https://www.victimsupport.org.uk/you-co/types-crime/online-crime/sexting/

online games and text communication platforms. According to research by the Global Initiative Against Transnational Organized Crime[20] the two most common forms of harassment in online gaming are *doxing* and *swatting*. *Doxing* is when one or more "online" participants request personal, identifying information about a particular user for the purposes of blackmail, or intimidation. *Doxing* can often lead to the publication of real names, phone numbers, home addresses, employer information and more. *Swatting* is a form of harassment that uses *doxing* techniques to create a real, tangible threat. The harasser reports the doxed user to local law enforcement, often claiming that there is a kidnapping or hostage situation at the victim's address, in order to intimidate, blackmail, and control the victim.

4.3. Investigating and Prosecuting ICT-facilitated Trafficking in Human Beings

In North Macedonia, the first case of online recruitment of a child by a paedophile was discovered as early as 2011.

Paedophile used Facebook to lure a child into having sexual intercourse, 2011
http://www.childrensembassy.org.mk/informator-br-40-ns_article-pedofil-preku-fejsbuk-namamil-dete-za-da-go-obljubi.nspx

Strumica resident A.T. (25) met a 10-year-old boy through the social network "Facebook" and after they agreed to meet, he lured him to go to another place, where he wanted to perform sex acts on him. The child's mother reported the case to the police. A criminal complaint was filed against A.T. for enticing a minor under 14 into having a sexual intercourse or other sex acts.
The investigation determined that on 18 March 2011, the suspect started communicating with the ten-year-old boy from the city through Facebook and began to persuade him to meet. The child accepted, so in the next three days he met the suspect twice. At the second meeting, on 21 March, A.T. persuaded the child to go near a church to perform sex acts. The child got scared and ran away, and subsequently told his mother about the encounter, who immediately reported the case to the police. Unofficially, this was not the first time the suspect had an encounter with children he met online.

[20] Глобална иницијатива против транснационалниот организиран криминал, Искористени пред нашите очи, Проценка на комерцијалната сексуална експлоатација на децата и одговорите за заштита на децата на Западен Балкан, Извештај од истражување, 2021, https://globalinitiative.net/wp-content/uploads/2021/05/Web-PDF-CSEC-Report-Exploited-in-Plain-Sight-Macedonian-final.pdf [Global Initiative Against Transnational Organized Crime, Exploited Before Our Eyes, Assessment of Commercial Child Sexual Exploitation and Child Protection Responses in the Western Balkans, Research Report, 2021, https://globalinitiative.net/wp-content/uploads/2021/05/Exploited-in-plain-sight-

More and more adults are contacting the First Children's Embassy Megjashi to report inappropriate photos on Facebook – the profiles are of adults or with children. They also have reports of video materials with sexual content from minors, with the intention to harm the reputation and dignity of another minor. Often, children use internet to directly communicate with strangers who have gained their trust, and even accept to meet with them. At the same time, the children and young people do not speak to their parents, but confide in the "friend from the internet" about their first sexual desires and experiences. In Megjashi, they also received reports about a recidivist, a person previously accused of sexual assault on a minor below the age of 14, who was still impersonating, deceiving and seducing children through Facebook, which was accordingly reported to the MoI.

Along those lines, and from the discussions in the round table[21] it became apparent that there is a great need to increase awareness of and knowledge about digital literacy for the use of social media of children and their parents. In parallel with digital literacy, it is also necessary to acquaint them with digital self-defence, that is, to teach them on how to protect themselves and how to prevent online child trafficking.

In 2022, a domestic case was discovered about exploitation of a child under the age of 14 by a THB gang. The girl got involved in the gang through her profile on the social network Instagram, and her photos offering and selling sexual services were uploaded on special websites.

An-assessment-of-commercial-sexual-exploitation-of-children-and-child-protection-responses-in-the-Western-Balkans-GITOC-.pdf]

21 Новите технологии и нивното влијание врз трговијата со луѓе – тема на дискусија на клучните чинители во Северна Македонија, 31.10.2023, https://www.coe.int/mk/web/skopje/-/new-technologies-and-their-impact-on-human-trafficking-discussed-with-key-actors-in-north-macedonia [New technologies and their impact on human trafficking – topic of discussion by key stakeholders in North Macedonia, 31.10.2023, https://www.coe.int/en/web/skopje/-/new-technologies-and-their-impact-on-human-trafficking-discussed-with-key-actors-in-north-macedonia]

First case: Girl under the age of 14 became a victim of online trafficking in human beings, 30.08.2022
https://mk.voanews.com/a/prv-slucaj-devojce-zrtva-na-onlajn-trgovija-so-lugje/6722522.html

A girl under the age of 14 became a victim of a Balkan network for online trafficking in human beings. She fell into the hands of predators through social networks. This is the first such case in North Macedonia.
The girl was seduced by a person who was part of a Balkan network for trafficking in human beings. The communication was carried out via the internet and social networks. Her photos ended up on the websites with sexual content.
The perpetrator was part of a larger criminal group, a network of predators - paedophiles. All the people who were in this network were adults (including people over fifty years of age) and they were asking children to do some horrible things.
The information and data that the law enforcement agencies received from the victim during the investigation were shared with Croatia (where the predator comes from) and Bosnia and Herzegovina (from where a person who approached the victims as someone who wanted to help her comes. He used a fake name, afterwards it turned out that he was a member of the group of online paedophiles/predators). There are on-going proceedings in Croatia and Bosnia and Herzegovina as well. The investigation in Croatia has been expanded in cooperation with the services from the United Kingdom.

In January 2023[22], the prosecutor in this case issued an Order against five persons who sexually abused a child and produced pornographic material. After the actions taken during the investigative procedure, the public prosecutor obtained solid evidence on which basis, in cooperation with the MoI NUSSMTHB an investigation was carried and searches were conducted on several locations in Veles, in Skopje and in Tetovo. Nine people were deprived of freedom, while one suspect was arrested from abroad. Six people were suspected of having committed the crime of child trafficking

[22] А1Он, Видео: Во случајот за сексуална злоупотреба на 14-годишно девојче осомничени уште десетмина, 30.03.2023 [A1On, Video: Ten more suspects in the case of sexual abuse of a 14-year-old girl, 30.03.2023], https://a1on.mk/macedonia/video-vo-sluchajot-za-seksualna-zloupotreba-na-14-godishno-devojche-osomnicheni-ushte-desetmina/

set out in article 418-d (418-г) paragraph 3 of the Criminal Code, 2 people were charged with the crime of Sexual Abuse of a Disabled Person set out in article 187 paragraph 2 in conjunction with paragraph 1, and 2 people were charged for the crime of Production and Distribution of Child Pornography set out in Article 193 paragraph 3 of the Criminal Code.

In another case, a 19-year-old male, who was in a relationship with a 14-year-old female, using psychological coercion, violence, blackmail and threats that he would share video materials with intimate content on social networks, forced her to have sex with adults for a certain amount of money on several occasions between 2022 and 2023. In the judicial proceedings, the accused admitted his guilt. On 8 May 2023, he was found guilty and received a prison sentence of 6 years imprisonment. The suspect was using the child's profile to communicate with the users of the sexual services provided by the child victim through Instagram.

Legal practitioners involved in the research affirmed that criminal proceedings involving child victims were specific and challenging. They are conducted in accordance with the legislation on juvenile justice. At the same time, minors very often change their statements or withdraw their reports, even when the child victim had his or her family support. Many potential THB victims detected by the mobile teams could not be identified as victims, so the suspects were not prosecuted, because proceedings are built solely on the testimony of the victims, which puts an enormous pressure on the victim, who is often vulnerable, and most probably traumatised. GRETA notes the same in its reports. GRETA was informed of several cases where potential victims have changed their testimony given to the prosecutor for various reasons (e.g., fear of a reprisal, a lack of protection and assistance, migrants' desire to leave the country as soon as possible) which led to a non-prosecution against the suspects or criminal prosecution for a minor crime. In November 2021, there was a case of two Syrian boys discovered by the police. According to the Kumanovo mobile team, the boys were sold and sexually exploited several times. However, the children changed their statements to the prosecutor, probably so they could continue their journey to EU countries, and the suspects were only charged with migrant smuggling.

There are also challenges when a child victim is questioned with respect to the evidence provided. Namely, the legislator provided certain procedural safeguards when it comes to examining a child victim, in order to avoid a re-victimisation. However, the lack of space and human resource (IT technicians), as well as the unavailability of technology did not allow the defence to follow the questioning of the victim and to be able to conduct

cross-examination, but the list of questions had to be previously submitted in writing. Thus, the court encountered allegations from the defence that there was no opportunity to ask the victim questions, that is, that there was no possibility for a cross-examination. In such a situation, the court is in a dilemma whether or not to accept such statements as evidence. Along those lines, the Convention on Action against Trafficking in Human Beings of the Council of Europe[23] is clear and requires the parties to adjust their judicial proceedings to protect privacy of the victim and guarantee his or her safety, including special procedural safeguards to protect child victims in criminal proceedings. In accordance with the European Convention on Human Rights[24] and the case-law of the European Court of Human Rights, in order to achieve such goals, it is fully permissible to hold hearings closed to the public, use audio-visual technology, recordings of the testimony and anonymous testimonies.

Reception centres for foreigners are extremely important in cases when there is a need for a temporary accommodation of foreigners when the conditions contained in the provisions of the Law on Foreigners are met, i.e., for housing foreigners who cannot be removed from the state territory within 24 hours, regardless of the reasons. Also, refugees and asylum seekers are susceptible to the risk of becoming THB victims, due to their status and the need to find a solution for their situation. That is why, a complementary approach to prevention is needed, that is, detection of the dangers before they happen. A significant aspect of this process concerns the humane treatment and protection of their rights, especially in cases where there are indicators suggesting that they may be potential THB victims. In this regard, it is imperative to apply due diligence and conduct comprehensive conversations with these individuals to gather information that may be of essential importance. The law enforcement agencies, and the immigration authorities should be actively engaged in assessing whether or not they may be THB victims by carefully examining their circumstances, their recruitment experience and their working conditions, and apply the relevant THB indicators.

The authorities should also investigate the method of recruitment, the communication channels used by the victims and traffickers (a communication platform/mobile phone application, social networks, e-mails, fora, etc.) and the method of exploitation. The THB identified victims can provide useful

[23] Council of Europe Convention on Action against Trafficking in Human Beings, Warsaw, 16.05.2005, https://rm.coe.int/168008371d

[24] European Convention on Human Rights, https://www.echr.coe.int/documents/d/echr/convention_ENG

information and evidence from the electronic devices can be extracted (photos, video recordings, messages, communication, etc.). In doing so, the appropriate legal procedures must be applied for the secured material to have value of evidence. The law enforcement agencies can use appropriate measures at their disposal, and especially through the application of ICT tools they can check and secure the necessary evidence, which will be important for further detection and investigation of this crime and perpetrators. The law enforcement agencies can obtain relevant information from the reception centres, medical facilities, non-governmental and international organizations that offer assistance and support to potential and identified THB victims (legal, medical, psychological, etc.). Therefore, the staff of the reception centres for foreigners should receive trainings on victims' identification in order to be able to effectively recognise the signs and indicators of ICT-facilitated THB and alert the competent authorities in good time. In view of the above, the practitioners from the law enforcement agencies also need language skills, considering that it is often a cross-border crime, and the members of the criminal gangs communicate in other languages and dialects, and often use coded communication. In view of the above, knowledge of the languages of the neighbouring countries, as well as of domestic dialects, including jargons, is particularly important for an easier and faster understanding of their communication.

There is also a challenge with begging, which is insufficiently and improperly processed through appropriate procedures. Often the crime is legally reclassified as "Child Neglect" as opposed to the documented case of child trafficking. Organized gangs involved in this crime have been observed by the authorities. For now, it has not been proven whether or not child trafficking for begging has been committed by misuse of ICT, despite of the well-known schemes in the region involving ICT.

5. Competent institutions for the use of ICT in the fight against ICT-facilitated trafficking in human beings

This section outlines the powers and responsibilities of the state institutions charged with detecting, identifying, prosecuting and investigating ICT-facilitated trafficking in human beings. In particular, the methods/tools, including ICT tools, available to law enforcement agencies in detecting and substantiating ICT-facilitated trafficking in human beings are presented and analysed.

According to the organisation and structure of the judicial system of the Republic of North Macedonia, the authorities in charge of combating trafficking in human beings are the Public Prosecutor's Office (in particular the Basic Prosecution for Organised Crime and Corruption), which has at its disposal the investigative centres and the judicial police (the Ministry of Interior (MoI), the Customs Administration (CA) and the Financial Police (FP)) and the judicial system (the basic, appellate courts and the Supreme court). Of course, as part of the investigation of such crimes, the Public Prosecutor's Office also receives information from other state authorities, such as the State Labour Inspectorate, the Financial Intelligence Office, centres for social work, health institutions, the Ombudsman, as well as civil society organizations and the media.

In January 2018, a Memorandum of Understanding was signed between the MoI and the MLSP for the establishment of the mobile teams. They were established in five cities across the country: Skopje, Kumanovo, Tetovo, Bitola and Gevgelija; they all have coordinators and several members. In February-March 2018, the "Work Programme of the Mobile Teams for the Identification of Vulnerable Categories of Citizens, including Victims of Trafficking in Human Beings" was drafted and adopted by both ministries. This multi-sectoral approach significantly contributes to strengthening the mutual coordination of the relevant stakeholders (MoI/MLSP/ civil society organizations), as well as for expanding the network of social workers in order to proactively identify THB victims. The role of the mobile teams is the application of a proactive and multidisciplinary approach aimed at vulnerable categories of persons as potential THB victims, so that they are promptly

identified and referred according to the procedures.

On 3 January 2018, the NUSSMTHB was established by the Memorandum of Cooperation on fight against organized migrant smuggling. It is concluded between the MoI and the Public Prosecutor's Office of the Republic of North Macedonia. This so-called "Task Force" was established in order to improve coordination and cooperation between the MoI and the Basic Public Prosecutor's Office for Prosecution of Organized Crime and Corruption of the Republic of North Macedonia. The NUSSMTHB is composed of police representatives from the central and local level, as well as focal points from relevant MoI units. It is a supporting pillar in the process of identification of the preliminary THB victims. The mobile teams and the NUSSMTHB contribute towards an increased number of detected potential THB victims among vulnerable domestic and foreign citizens, as well as migrants (from the migration influx) and their inclusion in the identification and referral procedures.

The Ministry of Interior, i.e. the police, through the appropriate organizational units, is in charge of detecting cases of trafficking in human beings committed with the help of ICT. Given the use of ICT in these crimes, the police can only access information by using appropriate ICT tools that will be able to oversee, monitor, detect and identify such behaviour on the internet. However, the research found that the police does not have enough adequate resources, capacities and modern technical tools to effectively execute their competences and conduct proactive investigations.

According to the 2022 US Trafficking in Persons Report[25] the law enforcement agencies investigated 1 case involving 3 suspects in 2021, compared to 6 cases involving 13 suspects in 2020. They also filed charges against 2 people in 2 cases of child trafficking for sexual exploitation, compared to 2020 when there was no such case. Courts convicted 1 trafficker *in absentia* for child trafficking for sexual and labour exploitation, which has been a significant decrease compared to the 9 traffickers convicted for child trafficking for sexual exploitation and 2 persons for child trafficking for sexual and labour exploitation. The trafficker was sentenced to 12 years imprisonment, compared to judges who handed down sentences ranging from 4 to 7 years to 11 traffickers in 2020. Courts of appeal upheld 2 convictions and overturned 1 conviction compared to 3 convictions upheld in 2020. The authorities were working with a limited capacity due to the pandemic, in accordance with the procedures for infected persons and for quarantine, and with limited human resources.

[25] 2022 US Trafficking in Persons Report, TIP Report 2022 - U.S. Embassy in North Macedonia (usembassy.gov)

The law enforcement agencies have launched joint investigations with the Greek and Serbian authorities and have cooperated as part of the Interpol investigation. There were cases when civil servants were accused and convicted: in 2022, a police officer was convicted of child trafficking, in 2017, a civil servant was convicted of complicity in trafficking in human beings, and in 2016, a municipal inspector was convicted of THB.

On the other hand, there are civil society organizations in the country that work on projects to provide assistance and support to the competent state institutions and THB victims. Some of them, also included in this research, are:

- The Journalists for human rights – created an information channel between the institutions (MoI, MLSP and MES) so that they can communicate more easily, they lead the Global passport project, the website www.najdi.org.mk, Amber Alert Europe www.amberalert.eu- it currently exists in some EU countries (France, Germany and Italy), in the region it is present in Albania (the USA version), and in North Macedonia where it is being implemented, the ownership will be in the MoI after 5 years. They are also in charge of implementing the Empowerment through self-defence project – an interesting approach that includes physical and mental exercises to strengthen children, which has already been successfully implemented in Albania.
- Macedonian Association of Young Lawyers[26] - have produced videos in Macedonian and Albanian to raise children's awareness about how predators operate on the internet and how cyberbullying and cyber trafficking take place. On www.kazistop.mk additional content has been published with advice to parents about their child's cyber presence.
- Semper[27] - since 2002, has been working on educational programmes for the prevention of various types of threats and dangers for children.

[26] https://myla.org.mk
[27] https://semper.org.mk

6. Human and technical resources to combat ICT-based trafficking in human beings

This section first presents and discusses the existing human resources of the institutions responsible for combating trafficking in human beings. These capacities are assessed based on the number of specialists in the respective units responsible for identifying and substantiating trafficking in human beings, the level of professional knowledge and expertise, the need to upgrade their knowledge and expertise, plans for investment in human resources, and completed and planned educational activities.

Given that these institutions have to investigate and build cases of ICT-facilitated trafficking in human beings, the research also analysed their technical capacities, that is, the availability of appropriate ICT equipment and relevant software tools for detection, investigation and identification of the perpetrators, as well as the need to upgrade their capacities.

Across various institutions within the law enforcement, including the inspection services, the survey revealed serious problems with respect to human resources. This issue has a dual nature, covering inadequate staffing and challenges related to the effective management of these resources.

First, there is a visible deficit in the number of professionals working in these institutions. This deficiency significantly hinders the operational capabilities to combat trafficking in human beings and related crimes. Limited manpower limits the ability to investigate, prosecute and resolve cases effectively, and thus creating significant gaps in their capacity to overcome this multifaceted problem.

A second notable concern refers to the frequent reassignment of staff within these organisations. The constant transfer of personnel from one organizational unit to another exacerbates the problem. When individuals are transferred to departments responsible for solving cases of trafficking in human beings, they often do not have the necessary knowledge, do not receive adequate training, do not have the sufficient expertise and experience necessary to deal with such complex and sensitive issues. This lack of expertise hinders the effectiveness of institutions as they deal with the complexity of THB cases without properly trained and experienced staff.

The consequence of these dual challenges is a reduced ability to effectively combat trafficking in human beings, while institutions struggle to optimally use their limited resources. For a comprehensive solution to these issues, it is imperative that efforts be directed towards increasing the number of qualified personnel and implementing strategies for the reasonable management and retention of these resources in the relevant institutions. This multifaceted approach is crucial to improving the efficiency of law enforcement and inspection services in their mission to combat trafficking in human beings and related crimes.

An additional problem is the lack of professional preparedness and specialisation in the field of ICT with advanced computer skills of the staff working on investigations in the field of trafficking in human beings. Until now, police officers have only had basic training on the online tools, but they have not had specific trainings that would enable them to collect information through open sources, monitor certain websites (such as employment sites), as well as launch initial proactive investigations. Cyber operations for identifying and detecting human traffickers can be lengthy and time-consuming.

The perception of members of the civil sector is that for the state "the technology is too expensive to put it in place in the institutions in charge of investigations". The education of the members of the law enforcement agencies about ICT and the method of gathering information and knowledge to substantiate the report of a THB ICT-facilitated case is insufficient. There are also no tools for early identification of victims.

According to the 2022 US Trafficking in Persons Report[28] BPPOPOCC, as in previous years, reported that they lacked the adequate staff and that there was a significant back log of cases, but that the authorities had increased the number of prosecutors from 10 to 13 to handle all cases under their jurisdiction. Despite not having a dedicated budget, the NUSSMTHB conducted proactive investigations, but continued to suffer from a lack of staff. The law enforcement agencies relied almost exclusively on the victims' testimonies without corroborating evidence. Local police officers lack sufficient knowledge on trafficking in human beings and have consistently failed to report potential trafficking cases to NUSSMTHB. Cases have not been thoroughly investigated or have been mishandled due to the absence of a digital case management system for reporting THB cases for various police services and prosecutor's offices. The authorities, with technical and financial support from donors, international and civil society organisations, have trained judges, prosecutors and members of the NUSSMTHB on various issues related to combating trafficking.

[28] 2022 US Trafficking in Persons Report, TIP Report 2022 - U.S. Embassy in North Macedonia (usembassy.gov)

In terms of technical resources, a lack of adequate technical equipment and software represents a significant and multifaceted challenge. This challenge arises from several key factors for institutions, such as high costs, the need for a continuous updating of the equipment and software, licensing agreements, as well as a lack of resources (financial, time, human) for training the staff who will use the equipment and software. The challenge of inadequate technical resources in the fight against ICT-facilitated THB is complex and encompasses financial, logistical and strategic considerations. While the need for advanced technology is clear, meeting this challenge requires careful management of resources, strategic planning, and potentially advocating for increased funding to ensure that the law enforcement agencies can effectively harness the power of technology in their efforts to fight THB.

Technology has a potential to aid law enforcement agencies' efforts to detect perpetrators of trafficking in human beings more quickly and easily and prevent them from harming potential victims in a timely manner. Tools for identifying activities related to trafficking in human beings, such as, for example, advanced operational monitoring, analytical tools, geographic mapping, drones for reconnaissance, surveillance and recording, etc., are continuously being developed. Online search tools, such as social media research or monitoring, are also quite useful. With them, the activities of certain user profiles can be passively monitored without any interaction, i.e., contact with the others. However, if it is necessary to establish contact, then it is a question of a covert operation, which implies a creation of a false profile and identity, active communication and interaction with predators.

Tech Against Trafficking[29] is a coalition of technology companies collaborating with global experts to help eradicate trafficking in human beings by using technology. Through their expertise, capacity for innovation and global reach, technology companies can play a major role in preventing trafficking in human beings and empowering victims. Digital information and communication technologies offer opportunities for change in tackling this crime. The existing technological solutions include mobile applications that help identify victims of sex trafficking; satellite images tracking vehicles carrying forced labour victims; and online research tools that collect images of child abuse to help law enforcement agencies find and rescue children.

In North Macedonia, among the law enforcement agencies and investigators, there are certain *ad hoc* activities for building capacities and appropriate ICT expertise for combating trafficking in human beings with the help of international partners and donors, based on the identified needs. However, there is no institutional and structure form of continuous and planned development and investment in the human, technical, information capacities.

[29] https://techagainsttrafficking.org/

7. Digital evidence - collection, securing, storage, protection, handling and processing

This section first provides a brief overview of the relevant standards for the collection, securing, and protection of evidence in a digital format that are specific and applicable to ICT-facilitated THB investigations. It elaborates the law enforcement policies and protocols for the collection, processing and analysing digital data from domestic and foreign providers and inter-agency cooperation and coordination in this type of investigations.

7.1. Digital evidence specifics

Digital evidence refers to any information, or data that is stored, or transmitted in a digital form and can be used as evidence in criminal proceedings. Digital evidence encompasses a wide range of electronic information, including text, images, videos, audio recordings, metadata, and more, that have been collected from a variety of digital sources.

Digital evidence has its own specifics. They exist in electronic, or digital formats. They are usually stored on electronic devices, servers, or in a cloud. They can be derived from a multitude of sources, including computers, mobile devices, social media platforms, online services, surveillance cameras, etc. When properly collected and preserved, they should remain intact and retain their integrity, so as to ensure their admissibility in the court. Digital evidence must be directly related to the case and have an impact on the issues being resolved in the legal proceedings. To establish their authenticity, digital evidence may require verification, so as to confirm that they have not been tampered with, altered or modified. Maintaining a documented chain of custody is crucial for monitoring the handling of digital evidence from its initial collection to its presentation in court, ensuring its reliability and credibility.

Digital evidence often includes metadata[30], which provide information about the creation, modification, and context of digital files. This metadata

[30] More information about metadata on the following link: https://www.britannica.com/technology/metadata, https://guides.lib.unc.edu/metadata/definition

can be significant in understanding the authenticity and time frame of the evidence. There are many definitions of metadata, but one of the simplest is that it is "data about data". More specifically, metadata (in the data management sense) describes a set of data about the following aspects: how it was collected; when they were collected; their geographic range; if there are multiple files, how they are related to each other; the definitions of individual variables and, if applicable, what are the possible options for them; calibration of any equipment used for data collection; the version of the software used for analysis; etc. Very often, a dataset that has no metadata is unintelligible. Metadata can be created, managed, stored and saved like any other data. There are three types of metadata: descriptive (consists of information about the content and context of the data), structural (describes the physical structure of complex data) and administrative metadata (used to manage the data).

Digital evidence can be subjected to forensic analysis, which involves specialised techniques and tools for extracting, preserving and interpreting data from digital devices. The admissibility of digital evidence in court proceedings is subject to legal standards and rules, which require their relevance, reliability and authentication. However, it is very important that the collection, security and handling and storage of digital evidence is done in accordance with the privacy laws and regulations in order to protect the rights of the individuals involved.

Why is it sometimes difficult to secure electronic evidence? Anonymous communication in the online space is extremely important to internet predators, that is, communication that has no traces and offers safe contact with people. Unlike connected networks and IP addresses that can easily be tracked and discovered, it is possible to establish a secure and anonymous contact using various tools[31]. The most famous of the tools is *Tor,* which was designed to allow anonymous use of the Internet, access to other software, including chat and email. Another possibility is *Tails* which is a completely separate operating system that is installed on a USB stick and can be safely used even if the usual operating system is hacked. Using *Tails* leaves no trace on the computer being used, unless specifically requested, and uses state-of-the-art cryptographic tools to encrypt files and emails. In addition to this, email encryption and secure email communication are possible and made simple thanks to the *Mailvelope* browser extension, which provides full encryption for an existing email address without changing the email client.

[31] Омазиќ, И., Дали може на интернет да се биде анонимен, 2020, [Omazić, I., Is it possible to be anonymous on the Internet, 2020], https://balkansmedia.org/mk/tutorijali/dali-mozhe-na-internet-da-se-bide-anonimen

Encryption and decryption take place exclusively on the end devices, which means that private data never leaves the device unencrypted. However, in order for the email correspondence to be fully encrypted, the "interlocutor" must also have *Mailvelope i*nstalled.

As revealed in the GRETA Study, in relation to encryption, the Slovenian authorities have raised the issue of the costs associated with the decryption of electronic data. It is costly to hire specialised, highly trained personnel, as well as purchase specialised software that can bypass the encryption. Furthermore, in parallel with the development of the encryption protocols, the software must be regularly updated, which often means considerable licence fees.

The key feature used to detect a suspect online is their IP address.[32] We are talking about situations where some criminal activity on the Internet can be linked to a given IP address and the goal is to identify the person with the IP address at the time when the criminal activity on the internet took place. However, the question can be asked the other way around, when there is an actual suspect and the IP address of the suspect used on the Internet must be found. The second situation is in many respects easier to deal with, because traditional investigative techniques (e.g., special investigative measures) can also be used. However, specifics in the detection of IP addresses and their association with perpetrators arise due to the Network Address Translation (NAT), the Carrier Grade Network Address Translation (CGN), the use of anonymisers (for a specific protocol: anonymous mail forwarder or anonymising proxy server, and independent of the protocol, such as TOR), as well as in the case of remotely controlling a computer infected with a botnet/ malware. After discovering the IP address, it should be associated with the username and the user, that is, the person with that username. However, usernames on some platforms can be easily changed at any time and are often used interchangeably by criminals, so it is difficult to determine who used that username at a given time.

An additional problem is created by online anonymisation softwares such as the VPN (Virtual Private Networks), which is designed to improve online privacy and security. These tools work by masking the IP address and encrypting internet traffic, making it more challenging for third parties to monitor online activities. Other anonymisation tools include *Tor*, proxy servers, browser privacy extensions ("HTTPS Everywhere" and "Privacy Badger"), secure messaging applications (such as Signal and WhatsApp that

[32] Training course for Judges and Prosecutors, Advanced course on the search, seizure and confiscation of online crime proceeds, Self-guided Training Manual, Council of Europe, 2017

offer encryption for messages and calls), and others. It is important to note that while these tools can improve anonymity and privacy online, their use should always be within the law and used for legitimate purposes only.

Another problem is that expert reports (on digital devices - computers, mobile phones, tablets, etc.) take longer, so, waiting for them to be completed, in order to be presented and submitted as evidence also delays the criminal proceedings. However, the presentation of these evidence before the court is also challenging. Such evidence is specific and complex and cannot always be easily understood by the parties in criminal proceedings. Therefore, they should be presented by experts who provide their expert opinion and the analysis in this regard. In the future, we should work on ways to explain and present such evidence by experts more clearly.

Digital evidence is a critical component of modern criminal investigations. It reflects the increasing role of technology in everyday life and the need for a solid and clear legal framework, as well as adequate capacities to manage electronic information in a legal context. In summary, all respondents agree that digital evidence represents a challenge for the law enforcement agencies in the world, as well as in North Macedonia, considering the following:

- their impermanence: (they can be easily manipulated, modified, deleted or damaged), they do not last for a long period of time (self-deleting messages with a particular timer released after a certain period or after viewing by the person to whom it was intended),
- their location: they used to be stored on floppy disks, then on CDs, on players, on USB sticks, and now with the development of technology they are located on various "streaming" services ("clouds"). It means they can, and most of the time they are, found outside the jurisdiction of the state. This entails the submission of appropriate requests for mutual legal assistance, or requests for obtaining information in an appropriate procedure by private companies, such as META or Telegram, Signal, Skype, Viber, WhatsApp, Twitter applications maintenance. When it comes to digital technology, there is a special place for the so-called *Darknet* which is a special layer of the internet, far larger than the publicly available, which is accessed using special protocols and applications *(Tor*). Originally conceived as a part of the internet that protects anonymity and prevents dictatorship, it has become a primary platform for criminal activity,
- a lack of a common general legal framework: since digital evidence is substantive evidence in which data and information (photos, videos, audio recordings, text and all other forms of information) are stored, received and transmitted in a binary form through electronic devices,

the real challenge is the drafting of written rules and procedures for the method of collection, protection from external influences, appropriate storage/warehousing, processing and analysing for the criminal procedure and their interpretation,

- human, technical and material resources and capacities: the insufficient training of the police officers, as well as a lack of appropriate technical equipment is an additional challenge.

7.2. Challenges in providing digital evidence of ICT-facilitated trafficking in human beings in North Macedonia

The law enforcement agencies in the Republic of North Macedonia face serious challenges during police investigations in detection, identification and documentation of ICT-facilitated THB and its perpetrators in terms of providing evidence in digital form. According to the respondents in the research, due to a legislative deficiency resulting in a lack of investigative tools, the investigative authorities do not have an opportunity to conduct secret (covert) online investigations (secret infiltrations) by, for example, creating fake profiles on the social networks whereby a suspect's involvement in THB can be investigated. This entails a need to purchase and access specialized software that will enable and document such investigations. Computer tools for accessing and downloading information from mobile phones and monitoring communication through various communication applications are also needed in this regard. Judges and other legal practitioners involved in the research consider such covert investigations, more specifically, the creation of false profiles a special investigative measure (SIM). Actually, in such a way, a false identity is created, which brings the risk of abetting a criminal offense, which is fully prohibited when applying SIMs. This way of controlling social networks and discovering a crime and its perpetrator(s) has been used in some countries of the region and has shown solid results. Legal practitioners, involved in the research, expressed doubts regarding the possibility and admissibility of such measures for the afore-stated purposes, and about their necessity. So, the lawful infiltration in the networks of predators to prove their online criminal activities, should be further discussed, as well as determined whether the existing legal solutions allow for their use or whether legal changes in the criminal law procedure should be introduced.

It should also be noted that the authorised officials of the law enforcement agencies who, although have official mobile phones, except for using them to make phone calls, cannot use them to collect evidence, for example, by taking photographs, recording videos from the scene of an event, for documenting traces, etc.

The Law on Criminal Procedure permits the use of special investigative measures in cases of trafficking in human beings, including communication monitoring, secret (covert) monitoring and the use of persons with concealed identities. In practice, the testimony of the victims still remains to be the main evidence of the prosecution, because the law enforcement authorities do not have sufficient technical, personnel and institutional capacities to collect other evidence. This significantly limits the capacity of law enforcement agencies to investigate trafficking in human beings, especially when it is committed by organized gangs or by misuse of ICT.

Still, law enforcement agencies may conduct an examination/search/data extraction procedure from mobile devices, so as to extract data that may have the value of an electronic evidence. This procedure for technical examination/search/data extraction from mobile devices, according to the relevant instruction[33] means the identification and storage of key artifacts that are normally available for viewing with appropriate software, and which in the future will serve to properly extract, analyse and preserve the data obtained by extraction from mobile devices. Following an order issued by a competent court or a public prosecutor's office, the police officer in charge of this procedure carries out a detailed identification of the digital devices that need to be confiscated and takes photos of the devices (invoices, manuals, the material from the packaging of the device, IMEI, MEID, ESN, MAC address, PIN and PUK and removable storage devices) in order to document the condition of each digital device that is being provided, which will further be subjected to analysis.

However, this procedure has its own challenges. So, for example, there are cases when investigators find a recording in a phone that was seized by order for the purpose of discovering and clarifying another crime, which proves that another crime was committed some time ago. At the same time, this evidence was not collected in a legal manner, but only the asset was confiscated in a legal way (with an order and with an issued certificate for temporarily confiscated items). In such cases, the lawyers request that such materials are not admitted as evidence. Consequently, the judge assesses

[33] Упатство за пребарување и извлекување на податоци од мобилни уреди, МВР, јуни 2022 [Guide for searching and extracting data from mobile devices, Ministry of Interior, June 2022]

whether the above is an indication or whether it will be accepted as evidence. In cases with the child victim, judicial practice accepts these materials as legal evidence with the argument that the victim is a child, and this gives a special quality and justification to this type of evidence.

According to civil society representatives, a major problem in reporting and substantiating cases of trafficking in human beings is that telephone conversations and photographs are not accepted as evidence in proceedings by the law enforcement agencies. Also, the recognition of persons through photo-documentation is not legally regulated and represents an additional problem for detecting perpetrators and providing evidence. Furthermore, data encryption is considered a difficult challenge, but so is the large volume of data and the rapid development of technology.

Securing computer data from ISPs that could constitute evidence in a particular criminal proceeding is not always straightforward. On the contrary, in most cases, what may be a priority for the domestic authorities, for the foreign Internet provider from where the data should be provided, this may not be the case. For the purposes of the criminal investigation, the following three types of data are usually required[34]: subscriber information, traffic data and content data. In many jurisdictions the requirements for access to subscriber information are usually lower than those for traffic data, and the strictest rules apply to content data. The type of data sought certainly affects the nature of the request to be made to an international service provider to gain access to the data. Some, but not all, international service providers have a form of rapid voluntary cooperation through which information about the subscriber can be provided while waiting for the formal legal process.

In recent years, such private Internet actors have taken on more active roles in law enforcement, especially in cases involving conflicts between the rights and freedoms of citizens, especially in the area of privacy. This is particularly reflected in the fight against illicit online content, including online sexual exploitation and ICT-facilitated trafficking in human beings, and the collection and securing of digital evidence by the law enforcement agencies. Each of these providers has its own regulations, privacy policies and protocols that comply with the legal framework of the country in which they are registered. Attempts at the global level to adopt common minimum standards and principles would facilitate communication between states and their law enforcement authorities with these companies. However, time, which may be one of the most significant actors in these proceedings, is not an ally of

[34] Training course for Judges and Prosecutors, Advanced course on the search, seizure and confiscation of online crime proceeds, Self-guided Training Manual, Self-Guided Training Manual, Council of Europe, 2017

the bodies that discover and prosecute the perpetrators of crimes. In these cases, it is necessary to act quickly and efficiently, but the communication and provision of information from the providers/companies often prevents this and appears as a factor that hinders the quick investigation. In any case, the uniform practice of the public prosecutors in coordinating the police and in submitting the requests for providing computer data is of exceptional importance for increasing the efficiency in dealing with these criminal cases. The Short Guide for Prosecutors[35] prepared with the OSCE support provides draft forms as a small contribution to such compliance in the procedure that can be useful for both public prosecutors and police officers. Considering that ICT and internet companies are developing very quickly, changing their privacy policies, protecting rights and regulating customer behaviour on their platforms requires further scanning of the situation and updating of this publication.

[35] Novakova-Zhikova, A. (ed.), Gathering Electronic Evidence from National and International Internet Service Providers, Prosecutor's Guide, OSCE, Skopje, 2017

8. Recommendations

Based on the findings and conclusions obtained from the conducted research, this section will provide the recommendations that could be used for future activities that contribute to sustainable capacity building, knowledge sharing and strengthening of expertise targeting key stakeholders (law enforcement agencies, prosecution, courts, lawyers, inspections, civil society organizations and media, social workers, etc.).

The GRETA's Study makes the following recommendations for detection, investigation and prosecution, which are also relevant for the authorities in North Macedonia:

- Law enforcement should invest in capacity building in the areas of Internet monitoring, cyber-patrols, undercover online investigations (cyber-infiltration), the use of OSINT by specialised officers, social network analysis, and the use of automatic searching tools to analyse evidence.
- Law enforcement and labour inspectorates should implement more stringent regulations and frequent controls on job advertisement websites. Labour inspectorates should develop digital expertise and increase their online presence.
- Countries/private providers/ civil society organizations must enhance online confidential reporting mechanisms, allowing anonymous reporting of THB cases as well as victims' self-identification. Countries should work with private companies offering online services to design out opportunities for traffickers, develop content analytics to detect THB instances and set up easily accessible mechanisms for clients to flag up suspicious activities/advertisements.
- Law enforcement should consider training officers specialised in both ICT and THB. Countries should also consider creating technical support groups staffed by sworn or non-sworn police officers with specialised ICT capabilities embedded within THB units.

- Law enforcement should make sure that all officers possess an adequate level of expertise in collecting and handling electronic evidence. Training on electronic evidence should be made integral to training curricula and constantly kept up-to-date due to the fast-changing technological and behavioural landscape. As the preservation of electronic evidence is key to building strong investigations, also counsellors and civil society organizations first-responders need to be familiar with strategies to preserve digital evidence (e.g., by storing chat histories).
- Countries/international organisations should regularly carry out a strategic analysis to generate knowledge on emerging trends on offenders' *modus operandi* as well as to keep up to date with the fast-changing behavioural patterns of technology users and the technological landscape. Based on this strategic evidence, countries can then launch targeted police operations, set up cooperation agreements, as well as devise targeted awareness-raising campaigns. Knowledge should be regularly disseminated at the national and supra-national levels.
- Countries should increase cross-border cooperation through streamlined procedures, the sharing of best practices and technologies (e.g., specialised software) and the enhanced dissemination of practical information about the contact points/ dedicated units that serve as "privileged contact" in the case of THB cases, including ICT-facilitated THB. Cooperation and support between destination and origin countries should be encouraged (e.g., expensive technological equipment might be affordable only to more affluent destination countries).
- Prosecutors should be provided with specific training on technology-facilitated THB and the handling of electronic evidence as well as its presentation before a judge/jury. Countries should take measures to ensure that prosecutors are familiar with procedures to request electronic evidence from private companies as well as obtaining evidence and cooperation from other countries both within the EU legal framework (via Joint Investigation Teams and European Investigation Orders) and outside the EU legal framework.
- Countries should develop data-sharing procedures with companies holding relevant data and consider developing cooperation protocols with private companies, including social network and gig-economy companies as well as rental platforms to foster the timely provision of information.

- A smoother process should be established for Mutual Legal Assistance Requests (MLAs), including clearer procedures, increased usage of enhanced networks of contact points, including European Judicial Network (EJN) contact points, and requirements for MLAs to be clearly set out and discussed at the outset. Countries should ensure that their personnel are adequately trained to process MLAs, EIOs and other international tools. Countries and international organisations should develop commonly agreed and accepted templates underpinning cooperation processes with a view to ease communication, decrease administrative burdens and minimise mistakes in the requests. Countries should also develop the use of secure forms of electronic communication and promote their adoption to smoothen international cooperation.
- Joint Training Activities (JTAs) should be envisaged for countries that are systematically engaged in joint THB cases. Transnational knowledge exchange can be fostered through participation in international/regional training focused on specific aspects of investigating ICT-facilitated THB. Such training should include case studies and scenarios on ICT-facilitated THB. Training on ICT-facilitated THB and associated legal instruments should also be provided to prosecutors and judges.
- Civil Society Organisations should receive training on the latest developments in both technological and THB landscapes, including changes in recruitment strategies. They should be in a position to exchange experiences on international best practices.

In addition to these recommendations, several other recommendations stand out. They relate to reporting, prosecuting and investigating, securing digital evidence and raising public awareness.

8.1. Recommendations for reporting

In order to improve anti-trafficking efforts and provide support to potential victims, first and foremost, accessible reporting tools and channels need to be established. For this purpose, **promotion and increased visibility of the online tool "Red Button" of the MoI is needed**. This online tool should definitely be more visible on the website of the MoI, in order to be easily

and quickly accessible, including the digital reporting assistance through the chat function, as it exists in other countries, but also it needs to be more accessible to the marginalized groups of citizens. Furthermore, a **telephone line exclusively dedicated for reporting cases of trafficking in human beings** needs to be introduced in order to be able to report anonymously and, if there is a need and an opportunity, to locate the victim through mobile operators. These two components are key to facilitating the reporting, intervention and assistance in THB cases.

Promotion and increased visibility of the Red Button online tool may include:

- **Awareness campaigns**: implementing a robust awareness campaign to inform the public about the existence and functionality of the Red Button tool. This includes using various media channels, social networks and community outreach efforts.
- **User interface**: this tool needs an intuitive and easy-to-use interface that encourages individuals to report suspicious activities related to trafficking in human beings, including a chat function, as well as reporting suspicious content on websites. This includes regular updates and improvements to make the tool more accessible.
- **Multilingual support**: Providing multilingual support within the application to accommodate users with different language backgrounds and to ensure that reporting is accessible to the general public.
- **Mobile application**: developing a mobile app version of the Red Button tool, making it easily accessible to individuals using smartphones and mobile devices common in today's digital landscape.
- **Partnerships**: cooperation with relevant government departments, civil society organizations and international organizations to promote the Red Button tool through their networks and resources.
- **Feedback mechanism**: implementing a feedback mechanism in the timely response tool and responding to user reports in a timely manner, ensuring that the public perceives the tool as effective and responsive.

The benefit of introducing a telephone line dedicated exclusively for reporting cases of trafficking in human beings is reflected through:

- **Dedicated hotline number**: establishing a toll-free hotline dedicated exclusively for individuals to call and report suspected cases of trafficking in human beings. This hotline should be open 24/7 to provide immediate response to emergencies.

- **Trained operators**: employing trained operators who specialize in dealing with THB cases. These operators should be equipped to provide information, support and guidance to callers while ensuring their safety and confidentiality. Ongoing training should be provided for the telephone line operators to keep them up to date with the latest trends and best practices in dealing with cases of trafficking in human beings.
- **Interagency cooperation**: coordination with law enforcement, social services and non-governmental organizations to ensure that reports received through the telephone line are dealt with promptly and that victims are provided with adequate assistance and protection.
- **Anonymous reporting option**: offering an anonymous reporting option to encourage individuals who may fear retaliation or legal consequences to provide appropriate and relevant information.
- **Public awareness**: conducting public awareness campaigns to inform the public about the existence, purpose and importance of reporting cases of trafficking in human beings.
- **Data collection and analysis**: collecting data on reported cases and analysing trends to improve prevention efforts, law enforcement strategies, and victim support services.

The combination of an accessible online reporting tool and a dedicated telephone line creates a comprehensive reporting infrastructure. This approach not only encourages the reporting of THB cases, but also ensures a quick and effective response, thereby strengthening efforts to combat trafficking in human beings and protecting potential victims.

8.2. Recommendations for investigation and prosecution

Regarding the legal aspects, **the existing legislation and the tools and instruments they allow to proactively detect persons who commit online stalking and sexual harassment need to be analysed and reviewed** in more detail. In developed countries this is achieved through conducting secret (covert) online investigations (covert infiltrations). Given that these types of investigations are not legally provided for, it would be necessary to initiate changes in this respect, taking into account the results they would give, and due to the increasingly frequent occurrence of the use of ICT for the recruitment and exploitation of victims, among which the largest number are children aged 7 to 13 years. This would certainly entail the procurement

of appropriate technical and information-communication equipment and training for the personnel - the investigators who will work on these problems.

In that respect, it is necessary **to sensitize the law enforcement authorities and the judicial authorities, the MoI, the inspection authorities, the public prosecutor's office and the courts, and inform them about good practices** that can be used in the detection and identification of cases of trafficking in human beings, their perpetrators and victims, but also in the prevention. That means:

- **learning from international and regional good practices** by exchanging experiences with other more developed countries on the use of ICT and learning from these comparative experiences through joint workshops, trainings and mentorships,
- **strengthening the investigative capacities of the law enforcement authorities** (by providing modern technical resources, ICT, expertise/knowledge) for identification, detection and documentation of cases of trafficking in human beings committed through ICT in order to more efficiently provide and collect quality evidence,
- **strengthening the preventive capacities of the law enforcement** (by providing modern technical resources, ICT, expertise/knowledge) for proactive research, early detection and identification of cases of trafficking in human beings and early warning by monitoring risky websites, controlling social networks and identifying suspicious job advertisements. In this respect is also the strengthening of efforts for proactive identification of THB victims and consistent checks for cases of trafficking in human beings among persons providing commercial sexual services, irregular migrants, refugees and other populations at risk,
- **developing specialized curricula** for conducting proactive investigations and providing, storing and analysing digital evidence. They should be included in into the regular curricula for initial and continuous training of the relevant professional groups, and especially for police officers, i.e., investigators. Prosecutors, judges, lawyers, experts and labour inspectors should be familiar with the possibilities and benefits offered by appropriate ICT tools in the process of detecting, identifying and substantiating trafficking in human beings,
- **increasing cooperation and exchange of information** between the law enforcement agencies, civil society organizations, ICT companies and other concerned actors for ensuring faster and easier detection of THB cases,

- **improving coordination between all authorities involved in the investigation** - there is no immediate response, effort and time has been invested in monitoring and collecting information and knowledge about the organised gangs, but without results. The existing cooperation protocols are not implemented,
- taking care **to protect personal data and private life of the victims** during and after the finalisation of procedures by removing the incriminating contents from the online space,
- **conducting joint multidisciplinary trainings** for all involved entities in cooperation with representatives of the civil sector in order to strengthen the cooperation between state authorities and specialised civil society organizations, because civil sector organisations still need to raise their awareness about the preventive role of ICT in THB cases.
- in order to gather evidence necessary for successful investigation and prosecution of cases of trafficking in human beings for the purposes of labour exploitation, it is also necessary to **strengthen cooperation between labour inspectors, other state and municipal bodies that perform inspections, investigators, mobile teams, trade unions and actors from the civil society**. In addition, the State Labor Inspectorate should have its own ICT facilities for safe storage and exchange of data with other relevant state authorities, given that it receives intelligence and information about potential cases of labour exploitation.

8.3. Recommendations for securing digital evidence

Regarding digital evidence, it is characteristic that their (im)permanence and location cannot be influenced, but it is important to insist **on drawing up clearly written rules and procedures for handling electronic evidence**, and familiarise all police officers with this. They will have to undergo **appropriate trainings for their implementation** and, of course, be provided with an **appropriate technical equipment for handling and storing electronic evidence**.

An **additional in-depth assessment by technical experts and an expert analysis of the existing technical resources** of the law enforcement agencies is needed, in order to determine the real needs for upgrading the capacities for detecting and investigating ICT-facilitated trafficking in human beings. Such analysis and assessment should provide a detailed picture of

the existing capacities and requirements for improving the capacities and increasing the efficiency of the law enforcement authorities.

To effectively investigate cases of ICT-facilitated trafficking in human beings, **investigators need to possess appropriate technical expertise and skills**. This could be part of the curriculum for their initial training on case investigation. First, they should be **proficient in digital forensics**. Experts should be able to acquire, store and analyse digital evidence from a variety of devices, such as computers, smartphones, servers and storage media. They should also **know the legal and procedural aspects of handling digital evidence**. Understanding network protocols, traffic analysis, and being able to trace digital footprints across networks is critical. This skill helps identify communication patterns between traffickers and their victims. Furthermore, **understanding cybersecurity principles** is essential to identifying vulnerabilities in digital systems that traffickers can exploit. Experts should know how to recover data from damaged or deleted digital storage devices. This skill can be key to finding evidence that traffickers may try to hide. **Proficiency in OSINT techniques and tools** for gathering information from publicly available online sources can help build profiles of traffickers, track their activities, and identify potential victims. **Understanding encryption methods and cryptographic techniques** helps to deal with cases where traffickers use encryption to protect their communications and data. Given the widespread use of smartphones, experts need to be **skilled in mobile device forensics**, including mobile device data extraction, mobile application analysis and recovery of deleted information. **Familiarity with the Darkweb and its platforms** is vital, as traffickers sometimes operate in hidden online space. Investigators need to know how to approach and navigate these areas while adhering to legal and ethical guidelines. They need to **understand social engineering tactics** and be able to recognise when traffickers use manipulation or deception to take advantage of victims or gain access to information. **Understanding cloud services** and being able to obtain evidence stored in cloud environments is becoming increasingly important, as traffickers may use cloud storage for data and communications. As technology evolves rapidly, experts need to be **committed to continuous learning** and be up to date on the latest developments in digital forensics and cyber security. All these technical skills, combined with a strong commitment to ethical behaviour and respect for legal procedures, give the computer crime experts the authority to conduct in-depth and effective investigations of ICT-facilitated THB.

Therefore, it is recommended to train at least two to three police officers, employed in the analytical services of the Departments of Internal Affairs,

the Regional Centres for Border Affairs, the Department for Suppression of Organized and Serious Crime, and the Criminal Police Department. The training should include methods of extracting electronic evidence from various technical devices according to orders provided by the public prosecutor's office. In parallel, it is also necessary to provide appropriate devices and software.

Furthermore, it is recommended to train at least three police officers from the NUSSMTHB, who, in addition to the training for extracting electronic evidence, will also undergo training for detecting persons who are using the internet and the ICT for "grooming". These police officers will need to be provided with the information technology with the appropriate software that enables searching by using certain phrases or words.

8.4. Recommendations for raising public awareness

The GRETA's Study makes the following recommendations in this respect:

- Private companies, working with the authorities and civil society organizations, should increase online social advertising to prevent victimisation and improve the detection of technology-facilitated THB. Countries should increase their efforts to inform individuals about their employment rights in a language they understand, in cooperation with civil society organizations and with companies that provide hosting services for job advertisements. The impact of campaigns should be routinely evaluated.
- Countries, civil society organizations and private companies that provide online and ICT services should run initiatives to raise awareness on technology-related risks, including how traffickers might exploit technology and how potential exploitative situations might begin. Schools and educators should be made part of this effort as children and young adults are exposed to heightened risks. Countries and civil society organizations should work with private companies offering communication and messaging services to design into the system information/warnings on the safe use of private channels of communications.
- Civil society organizations should offer training on techniques of data protection and safe use of technology as part of victims' protection and reintegration programmes. Victims should not be cut out of technology with the effect of disempowering them.

Raising public awareness of citizens about the seriousness of trafficking in human beings via the Internet is a multifaceted endeavour that includes consistent awareness campaigns and comprehensive media coverage. It should educate citizens on how to use social networks in a secure way, enabling them to recognise THB schemes and illegal immigration activities easily. An essential aspect of this effort includes the development and dissemination of promotional materials that are specifically tailored for students, teachers, and parents. These materials have a dual purpose: to raise awareness about the dangers lurking on the internet and to convey strategies for protecting oneself and loved ones from these digital dangers.

More specifically, awareness raising could be effectively achieved through:

- **Continuous awareness raising campaigns**: ongoing and strategically designed awareness campaigns are essential to informing the public about the indicators, risks and consequences of the ICT-facilitated THB. These campaigns aim to sensitize individuals to the existence of these issues in their communities.
- **Media engagement**: the media play a key role in disseminating information to a wider audience. Reporting cases of trafficking in human beings, including children, is particularly specific and sensitive. Journalists need training on now to report on and convey the appropriate information to citizens. Cooperation with different media channels ensures that the message reaches different segments of the society, reinforcing the importance of vigilance against ICT-facilitated THB.
- **Use of social networks**: social media platforms are powerful tools for mass communication. Using these platforms enables the dissemination of vital information, updates and resources to citizens, fostering collective awareness of potential risks and red flags.
- **Customised educational material**: tailored promotional materials should target specific groups of the general population. Materials designed for students, teachers, and parents can help address the unique challenges and vulnerabilities each group may face.
- **Emphasis on the internet security**: as part of these promotional materials, special emphasis is placed on the internet security. They educate individuals, especially students, about the dangers associated with the online interactions, such as cyberbullying, online predators, and the deceptive tactics used by human traffickers.

- **Cooperation with educational institutions**: partnerships with schools and educational institutions ensure that students and educators receive these materials directly, facilitating comprehensive and age-appropriate education about the internet safety and THB awareness.
- **Parental leadership**: recognizing that parents play a key role in guiding and controlling their children's online activities, educational materials should include resources to help parents initiate conversations about online safety and the risks of trafficking in human beings with their children and increase control over their online engagement.
- **Availability of resources**: these resources should be easily accessible, such as through online portals, community events or information sessions, so that citizens can easily access information and seek help when needed.

The essential goal is to have a well-informed and vigilant society by combining continuous public awareness initiatives, media engagement, and targeted educational materials about grave risks and serious harm caused by trafficking in human beings, as well as to find ways to protect the internet users from these occurrences. This multifaceted approach equips citizens, especially students, teachers and parents, with the knowledge and awareness needed to identify and protect themselves from physical and digital threats, fostering a safer and more resilient community.

Annex 1 - List of tech tools identified in the framework of the research

Category tools and forensics

No	Product	Link	Details	Observations
1	Maltego	www.paterva.com	Analysis	OSINT Application
2	Cellebrite	https://cellebrite.com/en/	Tool Subscription	Cellebrite is the go-to tool provider for mobile forensics, offering broad support of mobile devices and advanced data exfiltration. Cost
3	Palantir	https://www.palantir.com/	Tool. Subscription	Crime analysis
4	I2 Analyst's Notebook	https://i2group.com/i2-analysts-notebook	Tool Subscription	Crime analysis
5	Traffic Jam	https://www.marinusanalytics.com	Tool	Able to scan the internet and match trafficking victims with photos of missing children in sex ads
6	Thorn	https://www.thorn.org/	Tool	Child abuse
7	Project Vic	https://www.projectvic.org/		Scanning and removing content
8	Stop the trafficking	https://www.stopthetraffik.org	Platform	Reporting
9	Two Hat Security	https://www.twohat.com/	Platform	Dedicated anti-trafficking solution
10	Photo DNA	https://www.microsoft.com/en-us/photodna	Microsoft Tool	Help stop the spread of child exploitation
11	Child Exploitation Tracking System (CETS	Microsoft	Microsoft Tool	A software-based solution, which manages and links child protection cases
12	Computer Online Forensic Evidence Extractor (COFEE	Microsoft	Microsoft Tool	This kit helps computer forensic investigators extract digital evidence
13	Ship AIS	www.shipais.com	Locator	Locates ships
14	U Trace	www.utrace.com	IP Address	Geographical map location of an IP address

15	Geocode	www.geocode.com	Tool	Converts GPS coordinates to street address
16	Skye phone extractor	https://www.skyextractor.com	Data recovery	Data extractor
17	Tenorshare	https://www.tenorshare.net	Data recovery	Data extractor
18	DrPhone	https://drfone.wondershare.com	Data recovery	Data extractor
19	Wondershare Player	www.wondershare.net	Data recovery	Data wipe / Data recovery / PDF Editor
20	TRM Forensics	https://www.trmlabs.com	Forensics	Trace the source and destination of cryptocurrency transactions
21	Chainalysis	https://www.chainalysis.com	Tool	Reactor is the investigation software that connects cryptocurrency transactions to real-world entities
22	CipherTrace	https://ciphertrace.com/	Tool	Forensic analysis cryptocurrencies
23	Elliptic	https://www.elliptic.co/	Tool	Trace every transaction through the entire crypto ecosystem to gain a truly holistic view of risk.
24	Coinfirm	https://www.coinfirm.com/	Tool Subscription	is a valuable tool for businesses and governments looking to comply with AML regulations and combat money laundering.
25	Elliptic	https://www.elliptic.co/blockchain-forensics	Tool	Blockchain forensics
27	Magnet Axiom	https://www.magnetforensics.com	Tool. Analysis	used for high-level analysis
28	Velociraptor	https://docs.velociraptor.app/	Tool	open source tool designed for internal security teams to gather evidence across all endpoints
29	Wireshark	https://www.wireshark.org/	Tool	It can show every network packet sent from and received by a device
30	X-Ways Forensics	https://www.x-ways.net/forensics/index-m.html	Tool	a tool for investigators who like to manually dig deep for analysis, rather than rely on automation

31	CAINE	https://www.caine-live.net/	Forensics	Linux digital forensics distributions are available as virtual machines. These VMs include a number of tools pre-installed and preconfigured.
32	Infosniper	www.infosniper.net	IP Address	IP Address geoinformation
33	Camtasia Studio	www.techsmith.com	Capture	Screen recording and Video. Cost
34	Snag It	www.techsmith.com	Capture	Screen recording and Video. Cost
35	Atomic CD email extractor	www.massmailsoftware.com	Email	Locates email addresses from CDs and DVDs. Cost
36	Atomic CD email logger	www.atomic-email.com/email-logger	Tool	Locates email addresses from websites. Cost
37	Wireshark	www.wireshark.org	Analysis	Network protocol analyser
38	EnCase	https://www.opentext.com	Forensics	The shared technology within a suite of digital investigations products
39	Network Tools	www.network-tools.com	Network info	IP Address check and others
40	Rylstim	www.sketchman-studio.com	Screen movements	Record anything happening on screen
41	IP Address & Domain Info	https://addons.mozilla.org		IP Information
42	Autopsy	https://www.autopsy.com/	Tool	Autopsy is an open-source digital forensics software that gives investigators a full base to work from.
43	Screenshot	www.screenshot-utility.com	Tool	Capture onscreen image and send. Free
44	Swiftcodesinfo	www.swiftcodesinfo.com	Utility	Bank swift codes
45	Bindb	www.bindb.com		Bank Identification Numbers
46	OmniSCI	https://www.heavy.ai/	Tool	Analytics and Intelligence Platform
47	Geo Feedia	www.geofeedia.com	Analysis	Location based social media monitoring

Category search and general

No	Product	Link	Details	Observations
1	Google SSL	https://encrypted.google.com	Browser	Keeps search data from ISP
2	Torch	www.torchbrowser.com	Browser	Browser for torrent and other downloads
3	Tor	www.torproject.org	Browser	Access dark net
4	Memex	Registration	Browser	Dark web search engine
5	Duck Go	www.duckduckgo.com	Browser	Doesn't collect personal data
6	Copernic Agent Pro subscription)	www.copernic.com	App	Internet Search and Tracking tool
7	Global File Search	www.globalfilesearch.net		Local ftp sites
8	Document Search	www.documentsearch.org	Document	Document search by type
9	People Finder	https://www.peoplefinder.com	Identity	Search People
10	123 People	www.123people.com	Identity	Search People
11	Firefox	www.firefox.org	Browser	Search engines
12	Safari	www.safari.com	Browser	Yahoo based
13	Google	www.google.com	Browser	Search engines
14	Search by image	Google images	Browser	Search by images
15	Tube Surf	www.tubesurf.com	Video	Video
16	Blinkx	www.blinkx.com	Video	Video
17	Proxywonk	www.proxywonk.com	Anon	Fast free service
18	Gigablast	www.gigablast.com		Search engine
19	Untabbed	www.untabbed.com		Simplifies Google results
20	Instalooter	Package tools	Instagram tools	Download all pictures
21	Search Instagram	www.searchinstagram.com		Finds pictures on Instagram
22	Check Username	www.checkusername.com		Social Media
23	Yamli	www.yamli.com	Search	Arabic
24	Yandex	www.yandex.com	Search	Russian
25	Filecrop	www.filecrop.com	Shared Files	
26	Files Tube	www.filestube.com	Shared Files	

27	Search Shared	www.searchshared.com		
28	Twellow	www.twellow.com		Search public twitter accounts
29	FTK Imager	https://www.exterro.com/ftk-imager		Create forensic images of local hard drives
30	Sharedigger	www.sharedigger.com		Locates files in sharing and uploading sites
31	Similar Sites	www.similarsites.com		Website analysis tool
32	Similarweb	www.similarweb.com		Locates similar websites
33	Similar Site Search	www.similarsitesearch.com		Locates similar websites
34	More sites like	www.moresiteslike.org		Locates similar websites
35	OSINT Framework	https://osintframework.com/		A website directory of data discovery and gathering tools for almost any kind of source or platform.
36	Capture & Print	https://addons.mozilla.org		Print webpage
37	ArchiveFacebook	https://addons.mozilla.org	Analysis	Save Facebook content
38	RepKnight	www.repknight.com	Analysis	Social Media Management. Cost
39	Meltwater Buzz	www.meltwater.com	Analysis	Social Media Marketing software
40	Muster Point	www.musterpoint.co.uk	Analysis	Social Media Monitoring for LE and others. Cost
41	Babel X	https://www.babelstreet.com/		This international search system uses AI to cross language barriers for any search term. This is a cloud-based service
42	Google Dorks	https://www.exploit-db.com/google-hacking-database		OSINT data gathering method using clever Google search queries with advanced arguments.
43	Creepy	www.geocreepy.com		Gather geo info from social media
44	Exif Viewer	https://addons.mozilla.org		Metadata viewer
45	ProDiscover Forensic			

46	Cryptocurrency Forensics			
47	GeoTraceability (GeoSurvey, GeoTrace)			
48	SIFT Workstation			
49	Microsoft	Microsoft package for law enforcement		
50	Capterra	https://www.capterra.com	Toolbox	

Category contact details companies (for law enforcement)

Facebook

https://www.facebook.com/records/login/

WhatsApp

https://www.whatsapp.com/records/login

Telegram

https://telegram.org/privacy

Viber

https://www.viber.com/en/terms/information-for-law-enforcement-and-governmental-authorities/

Tik Tok

https://www.tiktok.com/legal/page/global/law-enforcement/en

Annex 2 – Questionnaires

Questionnaire for representatives of state institutions

Part 1. Impact of ICTs on THB

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

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

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

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

In your country, are ICTs used to facilitate financial flows in the context of THB? If so, in what ways?

To what extent are cryptocurrencies or cryptowallets used?

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

1	2	3	4	5
Very limited				Very important

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

Detection

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

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

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

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

Investigations

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

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

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

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

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

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

Prosecution

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

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

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

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

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

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

International Cooperation

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

Are there examples of good practices to enhance international cooperation?

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

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

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

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

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

Part 4. Leveraging on Technology

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

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

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

Part 5. Cooperation with private companies

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

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

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

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

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

Part 6. Cybercrime Convention (Budapest Convention)

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

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

Part 7. Protection of Human Rights

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

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

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

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

Further materials

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

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

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

Questionnaire for the CSOs

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

Part 1. The impact of technology on THB

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

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

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

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

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

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

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

Part 2. Using technology to fight THB

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

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

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

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

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

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

1	2	3	4	5
Very limited				Very important

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

Further materials

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

Questionnaire for Technology Companies

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

Part 1. Impact of ICTs on THB

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

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

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

Part 2. Cooperation with law enforcement agencies and civil society

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

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

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

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

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

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

Part 3. Leveraging on technology

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

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

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

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

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

Further materials

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

Questions for discussion in focus groups

1. Are there any challenges/problems/obstacles in the national legal framework for research (detection, identification, proof, documentation) of ICT-facilitated THB?
2. Please assess the current capacities and capabilities of the state institutions responsible for combating THB in terms of human and technical resources?
3. What are the victim identification and assistance procedures, if any?
4. What are the practical challenges in investigating cases of ICT-facilitated THB (challenges in the detection, prosecution, substantiation and international cooperation)?
5. Is there an established cooperation between state institutions and civil society and private companies in the investigation of ICT-facilitated THB cases?
6. How are educational activities related to the conducted ICT-facilitated THB research organized, if any?

Bibliography

- Глобална иницијатива против транснационалниот организиран криминал, Искористени пред нашите очи, Проценка на комерцијалната сексуална експлоатација на децата и одговорите за заштита на децата на Западен Балкан, Извештај од истражување, 2021, https://globalinitiative.net/wp-content/uploads/2021/05/Web-PDF-CSEC-Report-Exploited-in-Plain-Sight-Macedonian-final.pdf [Global Initiative Against Transnational Organized Crime, Exploited in Plain Sight, An Assessment of Commercial Sexual Exploitation of Children and Child Protection Responses in the Western Balkans, Research Report, 2021,
- https://globalinitiative.net/wp-content/uploads/2021/05/Exploited-in-plain-sight-An-assessment-of-commercial-sexual-exploitation-of-children-and-child-protection-responses-in-the-Western-Balkans-GITOC-.pdf]
- Заедничка декларација на министрите за внатрешни работи во Југоисточна Европа за јакнење на регионалната соработка во Југоисточна Европа за борба против трговија со луѓе, 16 март 2018 година [Joint Declaration of the Ministers of Interior of South-East Europe on Strengthening Regional Cooperation in SEE to Combat Trafficking in Human Beings, 16 March 2018]
- Закон за изменување и дополнување на Кривичниот законик, Службен весник на РСМ бр. 36/2023 од 17.02.2023 [Law on Amendments and Supplements to the Criminal Code, Official Gazette of the Republic of North Macedonia no. 36/2023 from 17.02.2023]
- 2021 US Trafficking in Persons Report, 2021 Trafficking in Persons Report - United States Department of State
- 2022 US Trafficking in Persons Report, 2022 Trafficking in Persons Report - United States Department of State
- Training course for Judges and Prosecutors, Advanced course on the search, seizure and confiscation of online crime proceeds, Self-guided Training Manual, Council of Europe, 2017
- Ла страда – Отворена порта, Можност или експлоатација, https://lastrada.org.mk/kampanji/mozhnost-ili-eksploataci-a/ [La Strada

– Open Gate, Opportunity or Exploitation, https://lastrada.org.mk/kampanji/2846-2/?lang=en]

- Новакова-Жикова, А. (ур.), Обезбедување докази во електронска форма од меѓународни и домашни интернет сервис провајдери. Краток водич за обвинители, ОБСЕ, Скопје, 2017 [Novakova-Zhikova, A. (ed.), Gathering Electronic Evidence from National and International Internet Service Providers, Prosecutor's Guide, OSCE, Skopje, 2017]
- Новите технологии и нивното влијание врз трговијата со луѓе – тема на дискусија на клучните чинители во Северна Македонија, 31.10.2023, https://www.coe.int/mk/web/skopje/-/new-technologies-and-their-impact-on-human-trafficking-discussed-with-key-actors-in-north-macedonia [New technologies and their impact on trafficking in human beings – topic of discussion by key stakeholders in North Macedonia, 31.10.2023,https://www.coe.int/en/web/skopje/-/new-technologies-and-their-impact-on-human-trafficking-discussed-with-key-actors-in-north-macedonia]
- Omazić, I., Is it possible to be anonymous on the Internet, 2020 [Омазиќ, И., Дали може на интернет да се биде анонимен, 2020], https://balkansmedia.org/mk/tutorijali/dali-mozhe-na-internet-da-se-bide-anonimen
- Пресечен меѓународен канал за трговија со луѓе од Тајван, 28.05.2021 [International Trafficking in Human Beings Channel with people from Taiwan Intercepted, 28.05.2021] https://jorm.gov.mk/presechen-me%D1%93unaroden-kanal-za-trgovi%D1%98a-so-lu%D1%93e-od-ta%D1%98van/
- Радио Слободна Европа, Тренчевска: Годинава три девојчиња биле цел на сексуална експлоатација, 30.05.2023 [Radio Free Europe, Trenčevska: This year three girls were the target of sexual exploitation, 30.05.2023], https://www.slobodnaevropa.mk/a/32435138.html
- Упатство за пребарување и извлекување на податоци од мобилни уреди, МВР, јуни 2022 [Guide for searching and extracting data from mobile devices, Ministry of Interior, June 2022]
- А1Он, Видео: Во случајот за сексуална злоупотреба на 14-годишно девојче осомничени уште десетмина, 30.03.2023 [A1On, Video: Ten more suspects in the case of sexual abuse of a 14-year-old girl, 30.03.2023], https://a1on.mk/macedonia/video-vo-sluchajot-za-seksualna-zloupotreba-na-14-godishno-devojche-osomnicheni-ushte-desetmina/

- Council of Europe Convention on Action against Trafficking in Human Beings, Warsaw, 16.05.2005, https://rm.coe.int/168008371d
- ECPAT International, Online child sexual exploitation: A common understanding, 2017, https://www.ecpat.org/wp-content/uploads/2017/05/SECO-Booklet_ebook-1.pdf
- European Convention on Human Rights, https://www.echr.coe.int/documents/d/echr/convention_ENG
- GRETA, Online and technology-facilitated trafficking in human beings, Full report, April 2022, https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49
- Latonero, M., The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking. University of Southern California, Annenberg Centre on Communication Leadership & Policy, 2012
- https://www.britannica.com/technology/metadata
- https://www.britannica.com/topic/sexting
- https://www.coe.int/en/web/anti-human-trafficking/greta
- https://www.plannedparenthood.org/learn/teens/bullying-safety-privacy/all-about-sexting
- https://www.verywellfamily.com/what-is-sexting-problem-1258921
- https://www.victimsupport.org.uk/you-co/types-crime/online-crime/sexting/
- https://guides.lib.unc.edu/metadata/definition
- https://myla.org.mk
- https://redbutton.mvr.gov.mk/default
- https://semper.org.mk
- https://techagainsttrafficking.org/

This publication was produced with the financial support of the European Union and the Council of Europe. Its contents are the sole responsibility of the author(s). Views expressed herein can in no way be taken to reflect the official opinion of the European Union or the Council of Europe.

ENG

The Member States of the European Union have decided to link together their know-how, resources and destinies. Together, they have built a zone of stability, democracy and sustainable development whilst maintaining cultural diversity, tolerance and individual freedoms. The European Union is committed to sharing its achievements and its values with countries and peoples beyond its borders.

www.europa.eu

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

www.coe.int

Co-funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Co-funded and implemented by the Council of Europe

IMPETUS

Center for Internet, Development and Good Governance

EU with YOU