Deliverable No 2.3
FOCUS GROUPS REPORTING

Project index number: 101101938
Call: ISF-2022-TF1-AG-THB

12/12/2023

Co-funded by
the European Union

Deliverable No 2.3
FOCUS GROUPS REPORTING

Project details

Keywords: trafficking in human beings, online investigations, judicial prevention, OSINT, digital hunting field

Project number: 101101938

Project Title: **INTERCEPTED ONLINE RECRUITMENT AND ADVERTISEMENT TO DISRUPT THE THB MODEL**

Project Acronym: INTERCEPTED

Coordinator: Prosecutor Office of Trieste (TSJudPol)

Call / Topic: ISF-2022-TF1-AG-THB

Type of action: ISF Project Grants

Project starting Date: 01/04/2023

Project end Date: 31/03/2025

Project duration: 24 months

Granting authority: European Commission-EU

Grant managed through EU Funding & Tenders Portal -ID: Yes (eGrants)

Consortium agreement: Yes

Deliverable Details

Number: D2.3

Title: Focus Groups Report

Lead beneficiary: Agenfor International

Work package: WP2

Dissemination Level: SEN- Sensitive

Nature: R – Document, report

Due date: November 2023

Submission date: December 2023

Authors:

Organisation	Author
Agenfor International	Naz Öztürk, Sergio Bianchi
KEMEA	Vagia Poutouroudi, Katerina Georgakopoulou
FUNDEA	José M. González Riera

Contributors:

Organisation	Author
TsJudPol	Antonio De Nicolo, Luca Petrocchi, Mario Melito, Pasqualino Brodella, Francesco Distefano, Marina Caneva

Version History:

Date	Version No.	Author	Notes	Pages (no.)
12.12.2023	1.0	Naz Öztürk	The first draft of the template has been shared with the partners for further adjustments and feedback.	
18.12.2023	2.0	Sergio Bianchi	General revision and adjustments have been made.	
18.12.2023	3.0	Naz Öztürk	The second draft of the template has been shared with the partners for further adjustments and feedback.	
20.12.2023	4.0	José M. González Riera	The final draft was revised.	

INTERCEPTED Project

INTERCEPTED (*Intercept Online Recruitment and Advertisement to disturb the THB Model*) aims to disrupt the digital business models of trafficker by strengthening the digital capabilities of law enforcement and judicial authorities in the framework of public-private cooperation, through a better and unbiased understanding of the phenomenon, an enhanced capacity to stay on-top of online trends from a technological and a policing perspective, and new tools for the detection and responses of recruitment for and advertisement of trafficked services online, fully exploiting the potentiality of the OSINT-HUMINT-SIGINT cycles.

The Focus Group is dedicated to exchange of ideas and practices focusing paying special attention to advertisement and recruitment to effectively intervene to both supply and demand sides of THB (Trafficking in Human-Beings). The event gathered Law Enforcement Agencies (LEAs), Internet Service Providers (ISP), Judicial Practitioners and Victim Protection/Assistance Services to discuss the following topics related to the INTERCEPTED project:

- The needs of different stakeholders involved in THB by understanding the key trends in recruitment and advertisement of trafficked services online.
- Existing trends in the recruitment of victims.
- The differences in the way that different victim profiles and purchaser profiles are targeted differently online, considering both the type of exploitation (e.g., sexual, labour, and if labour, in what sector, e.g., agriculture, textile, construction) as well as the specific traits of the victims, such as age (/broad age category), gender, nationality, disability.
- The ways in which different online platforms are used for the recruitment of victims of trafficking and the advertisement of their services.

The Focus Groups (FGs)

Each partner has conducted a Focus Group (FG) by November 2023.

The meeting lasted half-a-day for each FG depending on the participants, the coffee breaks, and the debate, which usually required more time than expected, thus highlighting the interest of the participants.
Informed consent has been granted before beginning the discussion. In addition, before the discussion the group members have been briefed about the topic of discussion and informed about their rights, including the confidentiality (e.g., that their identities will not be revealed in any report or publication).[1]

The entire sessions were recorded (audio or visual). There was also a note-taker who wrote down all important aspects of the discussion, but who was not a part of the discussion. This note-taker had in-depth knowledge about the topic at hand, and whose duty was to translate the notes taken during session into data for analysis. Areas of interest have been discussed during the session, moderated by the moderators appointed by the organizers prior to the session. The moderator made sure that all these areas have been covered during the discussion. He or she introduced new topics, directed the conversation, and encouraged participation while trying to minimize bias.[2]

The moderator created an environment that encouraged members to share their views, while keeping track of the discussion and preventing it from drifting from the topic at hand.[3]
The questions were open ended. However, there was a smooth transition from one question to the next. Each of the sessions started with introductory questions to address the general topic, helping the participants to understand the broader context. The general questions were followed by questions designed to elicit the

[1] Toolkit for Conducting Focus Groups. (n.d.). Retrieved from Rowan Education: http://www.rowan.edu/colleges/chss/facultystaff/focusgrouptoolkit.pdf
[2] Odimegwu, C. O. (2000). *Methodological Issues in the Use of Focus Group Discussions as a Data Collection Tool*. Retrieved from KRE Publishers: http://www.krepublishers.com/02-Journals/JSS/JSS-04-0-000-000-2000-Web/JSS-04-02-03-117-2000-Abst-PDF/JSS-04-02-03-207-212-2000.pdf
[3] Flick, U. (2006). *An Introduction to Qualitative Research*. California: Sage Publications.

specific information sought. The focus group ended with efforts to summarize the opinions of the participants.[4]

Finally, as the input from the FGs formed the basis of the forthcoming activities of project INTERCEPTED, it was compulsory for each FG Lead to take notes during the implementation of FGs and send it to KEMEA and AGENFOR approximately one week after the event.

[4] Magloff, L. (n.d.). Focus Group Technique. Retrieved from Chron: http://smallbusiness.chron.com/focus-group-technique-10741.html

Table of Contents

1. ITALY

1.1 Brief Description of FG Organisation:

On Friday 10th of November 2023, the Prosecutor Office of Trieste and Agenfor delivered the Focus Group (FG) titled: '*Nodes of public-private cooperation (PPP) in the context of* investigations into human trafficking'. The focus group meeting took place in a blended modality, in presence and on the Microsoft Teams platform, taking into account the participants' availability. In total, 21 (15 in presence and 4 online) first-line practitioners attended this meeting. More specifically, the meeting was attended by:

- 4 Police Officers
- 1 Public Prosecutor
- 2 Deputy Prosecutors
- 2 Judges
- 1 former Prosecutor
- 1 representative of EUROPOL
- 2 Directors of the Prosecutor Office of Trieste
- 1 Representative from an ISP
- 2 Representatives from NGOs
- 2 members of Agenfor's team
- 1 Officer supporting the Prosecutor Office of Trieste.

The focus group meeting started with a presentation of the INTERCEPTED project (objectives, outcomes, results). Then, the discussion focused on six main subject areas, according to the agenda.
The meeting lasted for 4 hours (with a coffee break).

1.2 Relevant Inputs, Key Results and Findings:

The first part of the meeting was dedicated to the legislative analysis, taking into consideration the new national and European legislation on the roles of Internet Service Providers and Hosting Service Providers as partners of the security and preventive policies.

The first speaker noted that in 2017, the EU Commission went beyond Directive 2000/31/EC and Legislative Decree 70/2003 with a communication on combating online offences and the role of ISPs (COM (2017) 555 final of 28.9.2017), defining the rules of conduct for the identification and removal of content even without waiting for orders from an administrative or judicial authority. In the regulatory landscape on combating the dissemination of terroristic content online, Directive EU 2021/784 – Legislative Decree 107/2023 has been analysed, which identifies hosting providers and content providers as actors involved in combating crime. The combined analysis of this legal framework provided several inputs for the INTERCEPTED project.

1.2.1 LEGAL PROBLEMS RELATED TO THE 'REMOVAL DIRECTIVE' EU 2021/784: THE ROLE OF INTERNET SERVICE PROVIDERS AND HOSTING PROVIDERS

Regulation No. 784 of the European Parliament and of the Council of 29 April 2021 – which became effective on 7 June 2022 – introduces the order to remove terrorist content posted online through the services offered by so-called 'hosting service providers',[5] whose sites could be used by third parties to carry out illegal activities, and more specifically by terrorist groups and their supporters to spread and propagate their message of recruitment and radicalisation of adepts or in order to organise, facilitate or direct terrorist activities. Its preamble refers to the responsibilities of hosting service providers vis-à-vis the company from the point of view of data protection against such unlawful use – while taking utmost account of the fundamental importance of freedom of expression and opinion – 'it lays down uniform rules to combat the misuse of hosting services for the purpose of disseminating terrorist content to the public' (Article 1). All these contents have been transposed into the Italian legal system through Legislative Decree No. 107 of 24 July 2023, but although it constitutes the legal text to which the Italian courts and administrative bodies will have to refer whenever confronted

5 "Hosting service provider" or "web hosting provider" means that company that owns and manages online platforms that allow, in fact, to 'host' content of different kinds (videos, image compositions, writings) uploaded there by thousands of users every day. Among the best known, for example, is YouTube, Facebook, Instagram, etc.

with the need to eradicate terrorist content from the web, or to prevent its dissemination, in applying it they will not be able to refer to the rules of the Regulation, especially with regard to the methods and timing of the execution of the removal order.

1.2.1.1 The essential elements of Regulation EU 2021/784

The removal order is the coercive measure by which the competent authority of each Member State of the Union requires a hosting service provider, which has its main establishment in one of the Member States, to 'remove terrorist content or disable access to terrorist content, effective in all Member States' if it is concerned to suffer its unlawful effects (Article 3.1)

- It must be reasoned and communicated to the recipient – through telematic and traceable transmission systems, capable of identifying the broadcaster with certainty and authenticity, at least 12 hours in advance, but once received, it must be carried out "as soon as possible and in any case within one hour of receipt" (Article 3.2), except in duly justified cases of emergency.
- It is then the obligation of the sender to indicate the means of appeal and the relative terms of proposition that the Regulations and the law recognise in favour of both the hosting service provider and the content provider (Article 3.4).
- Each hosting service provider having its principal establishment in a Member State must designate its own point of contact or, if that place is located in a State other than the Community, its legal representative (Article 15.1), which is subject to the obligation to inform, always by electronic and traceable means, the issuing authority of the execution of the order in all the Member States of the European Union, indicating the date and time.[6]
- Finally, it is very important to point out that the cross-border removal order must also be sent to the competent authority of the different Member State where the hosting service provider may have its main establishment, or its legal representative, since it is entitled to assess its formal and substantive legality and, failing that, to declare that it is ineffective, with a reasoned measure to be taken within 72 hours of its knowledge. In any case, this measure must be communicated to the issuing authority in advance.

6 In case of non-appointment of the legal representative 'all Member States shall be competent' (Article 16.2. See below).

1.2.1.2 System of appeals

The part of the Regulation and the law, in accordance with the principles of the European Convention on Human Rights and our Constitution, is that of the system of appeals, which is articulated through the three distinct institutes: the technical appeal, the review and the complaint. The appeal, which is of a judicial nature, lies with both the addressee of the removal order and the content provider and it must be brought before the courts of the Member State of the issuing authority. The deadline laid down in Legislative Decree 107/2023 is precisely that of 10 days from the receipt of the removal order.

The institution of the review, to which the persons referred to above are entitled and which must be proposed within 48 hours of receipt of the order before the court of the Member State where it has the principal establishment of the former or its legal representative. Within the next 72 hours, the Authority shall set out its conclusions on the existence of an infringement, informing that broadcaster, the hosting service provider, the content provider, and Europol.

If it has established the serious or manifest breach of its legal requirements, or the fundamental rights and freedoms guaranteed by the Charter, the removal order will cease to have legal effects, exactly as is the case in the case of examination of the removal order on the autonomous initiative of the Authority of the executing State referred to above.

Finally, the complaint institution, which is solely the responsibility of the content provider, and which must be addressed to the hosting service provider if it has spontaneously removed or obscured them by order of the Authority when terrorist content has been recognised. In this case, the hosting service provider must notify the hosting service provider of its decisions within two weeks and, if accepted, reinstate the content in question.

In any case, the hosting service provider is obliged to retain, through technical and organisational safeguards, terrorist content removed or whose access has been disabled spontaneously or following a removal order for a further period of 6 months, which can be extended, both in order to ensure the administrative and judicial remedies indicated above and for the purpose of preventing and investigating terrorist offences (Article 6 of Regulation (EU) 2021/784).

1.2.1.3 Obligations of Hosting Service Providers (including following the removal order)

Hosting providers are required to take specific measures to prevent terrorist content from being disclosed to the wide audience of the network and, although the Regulation ensures their wide freedom of choice regarding the precautions to be taken, Article 5.2 suggests some of them mainly focused on the adequacy of human and technological resources and on the ease of transposing any reports by users.
However, the assessment of the exposure of a hosting service provider to terrorist content does not belong exclusively to him; on the contrary, it is objectively configured by the Regulation that recognises it in the event that the one has received two or more removal orders in the previous 12 months.

It is important to remember that the removal of terrorist content does not imply its destruction. On the contrary, they must be kept in their integrity and in safety by the hosting service provider, both in order to allow any appeals to which it and the content provider are entitled, and above all to safeguard investigations and evidence acquisitions in respect of which those data are relevant.

1.2.1.4. The role of EUROPOL

The Regulation expressly provides for Europol's coordination and oversight role, not only to avoid 'duplication of efforts... and any interference with ongoing investigations in the different Member States', but also to ensure the adoption of effective and urgent security measures where certain terrorist content – which should primarily be detected and communicated to Europol by hosting service providers, through the contact point to whose designation they are required – should entail the threat of attacks on the lives of individuals or the integrity of a State.

Finally, it is recommended that a copy of the removal orders be sent to Europol in order 'to submit an annual report including an analysis of the types of terrorist content subject to removal or disabling orders' (see Articles 14.5 and 14.6).
Indeed, relations between the Member States and Europol have already proved to be a quick and effective tool to raise awareness among hosting service providers about specific content available through their services and to enable them to intervene quickly, remove it or obscure it on a voluntary basis.

The Regulation should be considered a *lex minus quam perfecta* because after having introduced the prohibition on the disclosure of terrorist content through the web, it provides only a financial penalty for the related violation, but not also the elimination of the act carried out in violation of that prohibition. The Italian Judicial Authority can remedy this contradiction through the seizure of computer data from the hosting providers referred to in Article 254 bis of the Italian Criminal Procedure Code (Italian Criminal Procedure Code), enforced by the judicial police or by prohibiting access to the internet domain while ensuring, where technically possible, the use of contents unrelated to illegal conduct (Article 7 of Legislative Decree 107/2023). Nevertheless, this procedure only applies within the territorial limits of the Italian State, except for its possible extension through a European Order of Investigation.

1.2.2 INDICATORS FOR THB: DIGITAL SOCIETY, NEW TECHNOLOGIES, AND HUMAN TRAFFICKING

Human trafficking is a criminal activity that has always been able to adapt and evolve quickly to changes in the economic, geopolitical, and social environment. This is also true with the advent of the digital society. Although the first reported cases dates to the early 2000s (i.e., a trafficker offering the sexual services of his victims to a large audience of potential clients through a website: UNODC, 2020), it is only in the last decade that the digitisation of human trafficking has become the focus of scholarly debates and a priority on the institutional agenda.

As noted earlier, the impact of the Internet and new technologies on crime and deviant behaviour is pervasive and multi-faceted (more so than commonly thought). The world of digital crime is not populated only by professional and experienced “hackers” who carry out complicated malicious attacks. Rather, they are rational criminal entrepreneurs who take advantage (to varying degrees) of the opportunities offered by the Internet and new technologies to facilitate or modify their traditional illicit work. At the same time, most criminal activity on the Internet does not take place in strange and encrypted virtual environments, but in public, on traditional websites, web forums, social media platforms, video sharing services, instant messaging applications, etc. This is also the case with human trafficking.

1.2.2.3 Recruitment in the digital society:

1.2.2.3.1 Misleading job-advertisements:

One of the main digital techniques used by perpetrators to recruit victims is the use of misleading job advertisements on trusted job portals, web forums, social media, and other virtual platforms. In some cases, traffickers are even able to create brand new fake job agency websites and promote such portals on social media to increase the number of visitors and potential victims.

This is a "fishing" technique in which traffickers make an initial pre-selection among those who respond to the advertisement: the perpetrators continue the subsequent recruitment phases (i.e., the fictitious agreement of the labour offer and transportation modalities) only with the profiles they deem most suitable for their purposes.

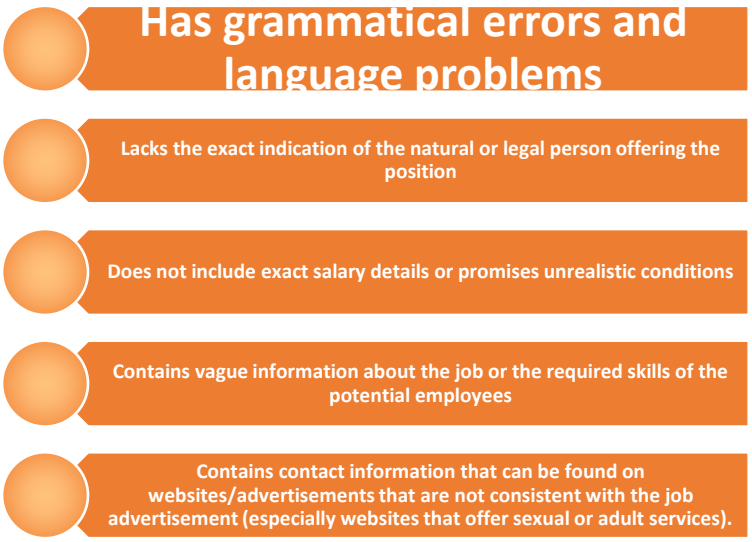


Table 1. Checklist. Indicators of possible fraudulent job advertisements hiding a human trafficking recruitment scheme (red flags). Source: Author's elaboration from the results of the Surf and Sound project.

In addition to the active recruitment technique described above, the Internet also provides traffickers with opportunities for a more passive form. It consists of the perpetrators scouring job portals, web forums, social media, and other classified websites for job offers from job seekers (especially abroad). Once a potential victim is located, the perpetrators conduct an initial interview and pose as a trusted employer looking to hire new employees. After this initial contact, traffickers typically charge the victim a fee to secure the job and help arrange travel and

accommodations. The victim does not discover the scam until they arrive at their final destination.

In this case, it is not possible to identify indicators because the entire recruitment scheme is carried out through the exchange of messages between the potential victim and the criminal. However, if there are known cases where a similar pattern exists, this should be considered and investigated further, as it could conceal a case of human trafficking.

1.2.2.3.2 The lover-boy Method (and other grooming techniques)

One of the most important roles played by the Internet is facilitating the so-called "lover boy method". This term refers to a traditional recruitment technique in which a trafficker feigns a romantic interest in a potential victim and seduces her with the promise of marriage (or a long-term emotional relationship) and a promising and better future by traveling abroad from her country of origin. It is a process of grooming and manipulation aimed at gaining the victim's trust, which allows the perpetrators to create a state of emotional dependence in which the victim is trapped. Then, as the relationship develops, and the victim reaches another location.

Even if social media are probably the most important virtual channel, other digital environments and platforms are also particularly suitable for the facilitation of the lover-boy method, i.e., dating services, web forums, and chat rooms. Furthermore, luring schemes may involve also other digital tools, such as online encrypted messaging systems (such as Telegram and WhatsApp)., traffickers begin to exploit the victim through physical or psychological coercion and methods of persuasion.

Figure 1: Explaining other methods of digital exploitation

1.2.2.4 How to spot fake job adverts: A guide by EUROPOL

What are they?

Fake job adverts are deceptive schemes where scammers post job listings to lure unsuspecting jobseekers into exploitative situations. They do this by posting attractive job listings from fake companies or by misrepresenting the working conditions. Once jobseekers arrive at the workplace, they find themselves in a completely different job or working under completely different conditions than those in the advert.

Who are the targets?

Fake jobs adverts tend to target anyone in a vulnerable economic situation looking for opportunities to improve their lives financially. Often the advertisements are for jobs abroad, further isolating the victims from possible support networks.

What to do if you or someone you know has become a victim?

If you have become a victim of labour exploitation or suspect that someone you know has become a victim, reach out to your national trafficking in human beings hotline or to the national police authority to report the situation.

Figure 2: A guideline to spotting fake job adverts

1.2.2.4.1. How can you protect yourself?

When searching for jobs, beware of advertisements that sound too good to be true – they are usually.
Take the Following Preventive Measures:

- Do a background check of the company to ensure it is a legitimate entity and has no reports of violating labour regulations.
- Do a background check on the presumed recruiter or manager of the company.
- Critically examine the job advertisement's details and conditions. Are they too good to be true? For instance, are the promises of the job and salary conditions realistic? Do they correspond to going rates in the market in question?
- Look for obvious grammar and spelling mistakes in the job advert.

1.2.2.4.2. How does it work?

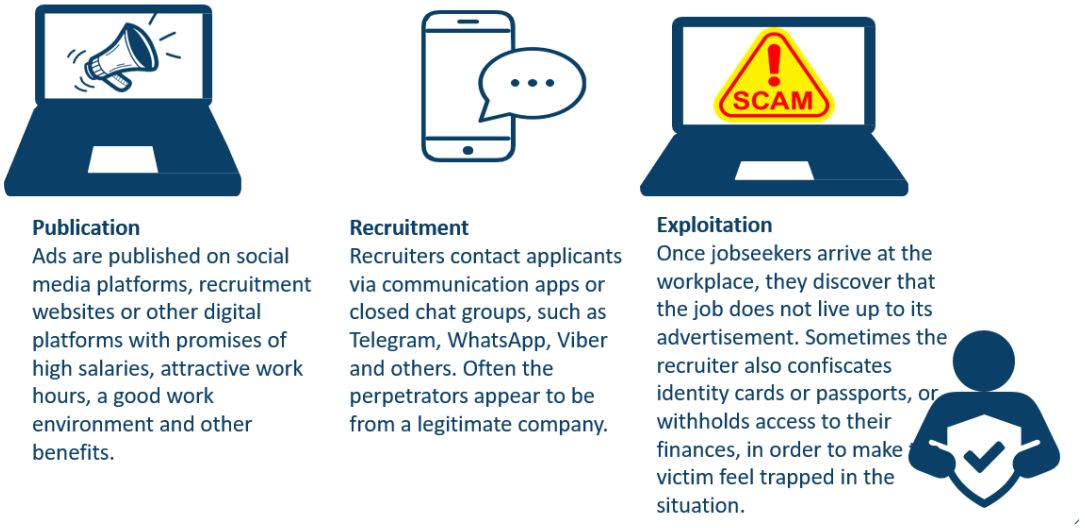


Figure 3: Figures explaining the steps of exploitation

1.2.2.5 Victims-centered approach

1.2.2.5.1 Well-being, protection, and security first:

This initial principle is based on "do no harm", and aims to prioritize the well-being, rights, and dignity of the victims. The responsible parties should make sure that the victims feel secure and implement the necessary security measures to prevent retaliation, re-victimisation, and re-traumatisation.

1.2.2.5.2 Assistance and support offered to victims:

Assistance and support should be offered to all victims of human trafficking, irrespective of whether the victim initiates or is willing to cooperate with the ongoing investigations or not. The support should follow an opt-out model, where the service providers assume consent until the victim officially takes action to revoke permission.

1.2.2.5.3. Non-discrimination

Within the human trafficking victim's context, non-discrimination principle is prominent to uphold. Non-discrimination means that every victim, irrespective of race, skin colour, sexual orientation, gender identity, language, religion, political or other opinion, national or social origin, property, birth, health or other status, or any other characteristic, is entitled to receive the most appropriate response to their circumstance.

1.2.2.5.4. End-to-end, holistic approach

The end-to-end approach entails that the assigned appropriate assistance will be delivered to the victim from the beginning to the end. The process starts naturally with the detection of the crime, then continues through the proceedings and ends with a potential conclusion connected to the crime. According to the victim's situation, the support can go beyond the conclusion of the proceedings, official or not.

1.2.2.5.5 Give (back) a measure of control to the victim, to the feasible extent

The victims must be given a measure of control in terms of the information they decide to disclose, alongside within the course of the assistance they are receiving and the proceeding they are undertaking with the concerned authorities. If there is the necessity to undertake proceedings or actions in which the victims disagree with, the victims should be properly informed as to why the course of action is necessary.

1.2.2.5.6. Confidentiality and informed consent

The clear meaning and scope of these concept must be disclosed to the victims as early as possible, ideally before the victim starts to share personal information and throughout any proceeding to follow.

1.2.2.5.7. Ask and listen

It is prominent to create an environment of trust with the victim, which would initially start with the assumption that the victim is not guilty, therefore listening to the victim without bias or judgement. It is equally important to approach the victim with empathy, starting with the possibility that the occurrences communicated by the victim may have happened.

1.2.2.5.8. Information - Keep the victim informed

The victim must be timely informed on any outcomes or developments which concerns the victim, throughout all the processes and actions undertaken. If relevant, the victim must be clearly informed as to why some types of information cannot be shared or cannot be immediately shared with the victim. It is also important to communicate with other entities engaged to ensure the accuracy of the information provided in a coordinated manner, while respecting boundaries of consent and confidentiality.

1.2.2.6 Child Victims

The support and assistance provided to the victims below the age of 18 are undertaken per Article 3 of the Convention on the Rights of the Child (CRC), prioritizing the "best interest of the child. The term 'best interests of the child' broadly describes the well-being of a child. "A variety of individual circumstances determine a child's well-being, being the age, gender, level of maturity and experiences, as well as other factors such as the presence or absence of parents, the quality of the relationships between the child and family/ caretaker, the physical and psychosocial situation of the child, and her/his protection situation (security, protection risks, etc.)." Finally, the children must be able to express themselves in parallel with the level of their maturity.

1.2.2.7. Due Process

The due process of the alleged perpetrators must be explained to the victims as soon as possible, to enable the victims to understand how the perpetrators proceedings might affect her/him.

1.2.3 INTERNET SERVICE PROVIDERS AND HOSTING PROVIDERS AS PRE-INVESTIGATIVE AND INVESTIGATIVE AIDS

ISPs offer services of:

- Access Providers (e.g. offer Internet access)
- Service Providers (e.g. offer e-mail)
- Content Providers (they offer their own content)
- Caching (they offer content, cache, to optimise performance)

Host Providers (host content from others)

- and functions of:
- Hosting: services managed by the provider
- Housing: services managed by the customer

1.2.3.1. ISPs and their responsibilities

The Responsibility Scheme of Internet Service Providers is laid down in Directive 2000/31/EC, transposed in Italy by Legislative Decree 70/2003 which types the activities of ISPs into three categories:

- Mere conduit provider (Article 12): simple transport activities.
- Caching provider (Art. 13): automatic, intermediate, and temporary storage activities.
- Hosting provider (Article 14): information storage activities.

Article 15 of the Directive, entitled 'Without the general obligation to supervise', which finds a parallel in Article 17 of Legislative Decree 70/2003, regulates limited liability for monitoring information (transmitted and stored).

From the point of view of the protection of personal data, EU Regulation 679/2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC

(General Data Protection Regulation), does not prejudice the application of Directive 2000/31/EC, in accordance with Article 2(4) of Regulation 679/2016 EU.
In this regard, it is appropriate to recall the Judgment of the European Court of Justice – Grand Chamber – 13 May 2014, in the proceedings against Google Spain, which confirms the non-applicability to ISPs of liability or control over the data stored or transmitted while there is an obligation to delete the contents by the controller.

However, with (COM (2017) 555 final of 28.9.2017), the EC defined a set of rules of conduct for the identification and removal of content even without waiting for orders from an administrative or judicial authority. In the regulatory landscape on combating the dissemination of terroristic content online, there is Directive EU 2021/784 – Legislative Decree 107/2023 which identifies hosting providers and content providers as actors involved in combating crime and establishes:

- Removal of illegal content within 1 hour of PM notification
- Administrative sanctions: from EUR 25.000 to EUR 300.000
- Criminal sanctions: shutdown and up to 4 % of ISP worldwide turnover

1.2.3.2. ISP – pre-investigative aids

ISPs can provide critical collaboration during the pre-investigative phase to gather information to understand ever-changing criminal scenarios.

The means of achieving these objectives are essentially:

- In the provision of appropriate digital infrastructures (e.g.: network, cloud).
- In the use of appropriate OSINT (Open-Source Intelligence) licenses.
- In the equipment of Platforms for data analysis.

1.2.3.3. ISP – aids in the investigation phase

ISPs following the measures of the Judicial authority are required to provide any useful information in order to identify the perpetrators of possible crimes.

In the case of computer breaches, ISPs are required to provide the necessary material, such as traffic flows, data regarding the investigation, information on the subjects who have visited certain web pages and, in general, all data required by

the judicial authority. To provide this information, appropriate digital infrastructures and data analytics platforms must be used.

1.2.3.4. What is the winning model?

The Public-Private Partnership Model represents a sure-fire success in combating online crime, founded on cooperation established during "peace times" (prior to the emergence of the phenomena described in the online context) between public entities responsible for the fight against illicit activities and well-versed in such phenomena, and private entities providing digital services that may be misused for unlawful purposes.

Specifically, the public sector is acknowledged for its domain competence, possessing knowledge of dynamics, patterns, processes, and related aspects. On the other hand, the private sector brings technical expertise, leveraging its knowledge of technologies. Through this collaboration, it becomes not only possible but necessary to develop data correlation models to address the issues described above.

However, the activity highlighted the difficulties to involve ISPs/HSPs in preventive and judiciary activities, while recognized that CSOs and NGOs have a more proactive attitude to the public-private cooperation in this field.

As output for the future actions, the meeting considers the importance to dedicate extra effort to strengthen cooperation between ISPs/HSPs, NGOs/CSOs and public institutions in the field of justice and security as a key to prevent THB-related crime.

1.2.4 ASPECTS OF EUROPEAN CRIMINAL COOPERATION IN THE FRAMEWORK OF THE PP

1.2.4.1. Deputy Prosecutor

Analysing financial flows from Europe to countries of origin and establishing information hubs are crucial aspects for addressing the discourse on European criminal cooperation within the Public-Private Partnership (PPP) framework. Furthermore, these aspects are intricately linked to the theme of cross borders, specifically how evidence is acquired abroad and the way it is utilized in legal proceedings. This consideration arises from the understanding that prevention is highly valuable, but procurement should come into play only after civil society once international systems and other protective measures have been activated.
Trafficking investigations exhibit two distinct characteristics: the examination of individuals facilitating the passage and scrutiny of the final terminal—those who activate exploitation not as an external entity to the chain but as integral members of an organization familiar with the various stages from recruitment to the final terminal.

Addressing the issue of exploitation necessitates a consideration of nationalities. Specifically, trafficking investigations inherently involve activities occurring abroad. Therefore, even when an individual transits through Italy enroute to another destination, it becomes imperative to analyse their passage within Italy. Ultimately, the exploitation of an individual implies that this act occurred abroad. The utility of this information in international judicial cooperation is ensured through various available mechanisms. However, despite the inclusion of the Judicial Police in an investigation, the data acquired from these mechanisms cannot be employed, even during the trial stage or when requesting the Preliminary Investigations Judge to grant a precautionary measure. Nonetheless, thanks to EU international judicial cooperation, the search for evidence abroad is facilitated.

During the recruitment and journey phases, as well as in the sorting phase, social networks play a crucial role. This is augmented by the additional dimension of e-trafficking, involving encrypted chats (such as Sky, etc.). Penetrating these encrypted chat systems equips investigators with the ability to uncover traces of past conduct.
Remaining in the digital realm, the analysis of money transfers, especially within a payment system built on trust among traffickers, is significant. Migrants are required to relinquish their money at the time of departure to one of these

individuals based on a fiduciary relationship (word of honour). A system of calculating payments through debit/credit compensation ensures that, at the end of the payment chain, there is no substantial transfer of money. Instead, compensations result in a singular traceable passage of money.

The challenge lies in how to present this data in a useful format for judicial proceedings. This intersection between the public and private sectors serves as the linchpin for addressing this question.

1.2.4.1.2 Judge for Preliminary Questions

New interpretative guidelines regarding the facilitation of illegal immigration must undergo testing. Currently, there are forms of judicial cooperation with Libya, Egypt, Tunisia, and Turkey that, despite yielding varied results, have never been neglected due to some positive outcomes. Simultaneously, collaboration with EU agencies, particularly Frontex, is available.

Within the realm of cooperation, the significance of 'technological proof,' i.e., evidence acquired through technology and connectivity, is recognized. This often helps corroborate initial evidence. The primary focus of law enforcement action is to intercept, block, and target medium-high segments of organizations dedicated to aiding illegal immigration (such as blocking ships in international waters, asserting Italian jurisdiction, and guiding ships to port).

Fundamental to these efforts is the initial observation activity in international waters involving photos, seizure of phones and on-board equipment, and data collection from the phones of involved parties. In certain cases, interceptions involved leaders of organizations in Egypt and Libya communicating with individuals in logistic bases in Italian territory, providing valuable insights into their modus operandi.

Equally important is exposing and acquiring testimony from migrants, particularly those willing to collaborate and share their experiences. These steps then undergo procedural scrutiny.
In practical cases, the Anti-Mafia District Directorate (DDA) adopted an approach involving small working groups with specialized Public Ministries (PMs), creating connections with local prosecutors. Every communication of crime news (CNR) was shared with the District Attorney's group dealing with these crimes. Probationary incidents were promptly addressed, leading to the identification of

leaders in Egypt, Libya, and Turkey. Judges for Preliminary Investigations (GIP) with custodial ordinances activated forms of rogatory (Palermo Convention) with varying outcomes. While Egypt and Libya cooperated in identifying certain subjects, boats, or telephone numbers, objections were often raised when foreign countries were asked for the surrender of individuals.

Despite negative responses, dialogue with judicial authorities in these countries persisted. Measures to contain departures were eventually adopted, and collaborative activities in oil smuggling between Italy and Libya were established. The final realization is that logistical bases are established in these countries, and they must independently muster the forces to activate their own investigations. Family-based and friendly micro-organizations exploiting prostitution contribute to migrant smuggling and bring thousands of people to Italy. Coordination between district prosecutors and international public and private agencies, such as UNHCR, led to the formation of a specialized group studying the changing cycle of migration flows.

Trafficking in people differs from the facilitation of illegal immigration. In smuggling, most activity occurs in the countries of origin before the sea voyage, while for trafficking, exploitation must occur in the destination country. Monitoring work, involving specific protocols among prosecutors, Prefectures, anti-mafia and anti-trafficking agencies, and reception facilities, is crucial to report young people destined for trafficking pathways to competent district prosecutors. Digital data has facilitated corroborative information around the victim, utilizing social profiles, open sources, GPS tracking, and technological proof. Collaboration is not impossible, as Eurojust, an agency for judicial cooperation in criminal matters, acts as a facilitator and a dialogue hub with third countries, including liaison officers with agencies such as Europol. Confronting Eurojust before initiating cooperation activities is vital to understanding the most appropriate cooperation path for specific circumstances and countries.

1.2.4.1.3. European Migrant-smuggling center: EUROPOL

An example of action to combat human trafficking is given by the PHOENIX Analysis Project against the Trafficking in Human Beings whose activities began in June 2007. The project team is made up of specialists who operate on a dedicated database: 27 EU (MS) and 11 Non-EU (TP) (AL, AUS, COL, DK, EJ, ICE, IP,

MOD, NO, SB, CH, UK, USA CBP-DSS. Since 2011, THB has been a top priority for EU police forces.
In summary, the project allowed to:

- Provide analytical and operational support to high profile cases.
- Developing knowledge on trafficking in human beings in the EU.
- Support EU law enforcement policy approach against trafficking in human beings.

1.2.4.1.4 Further trends and challenges:

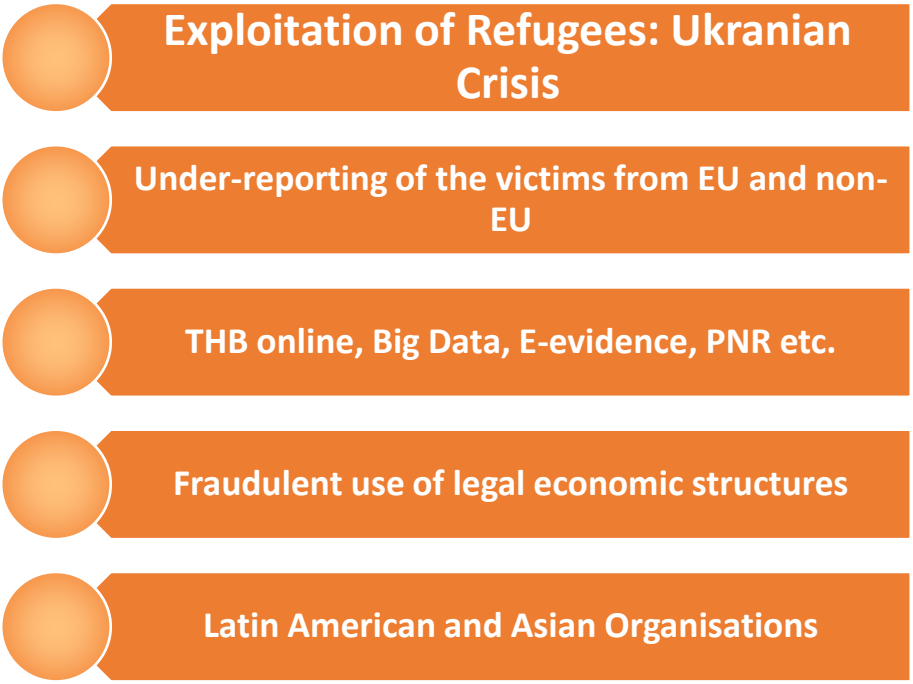


Figure 4: A summary of the current trends and challenges

1.2.4.1.5 Cooperation with the private sector:

Cooperation between law enforcement and the private sector is crucial in the fight against human trafficking. This is because private actors possess unique knowledge of their sectors, placing them in a key position to gather information and develop innovative measures to prevent and counter criminal exploitation attempts. Examples of private actors include NGOs, financial institutions, internet service providers, and tourist/temporary rental platforms. Civil society and NGOs

play an important and complementary role in the timely identification of victims and the initiation of investigations.
In this context, the role of Europol, established by REGULATION (EU) 2016/794 on 11/05/2016, most recently amended by REGULATION (EU) 2022/991 on 08/06/2022, regarding Europol's cooperation with private parties, Europol's processing of personal data in support of criminal investigations, and Europol's role in research and innovation, deserves attention.

1.2.4.1.6 Europol Regulations Comparison

Comparing both mandates, according to the new regulation the following could is valid[7]:
Europol may receive personal data directly from the private sector in order to identify the countries concerned with two exceptions:

- In case of major cyberattacks (art.26a) or online dissemination of material (art.26b), Europol may enrich the information received from the private sector by processing it and comparing it with its data in order to find links to ongoing criminal investigations.
- Europol may make its structures available to facilitate cooperation between the competent national authorities and the private sector (Article 26.6c)
- Europol may require Member States, in accordance with national laws, to obtain personal data from private parties (Art. 26(6b), 26a(6) and 26b(6)).

1.2.4.1.7 PPP: Areas of Interest

Therefore, in the light of the principles set out below, Europol's public-private partnerships may address the following areas:

- Anti-money laundering and terrorist financing.
- Cybercrime.
- Child pornography.
- Cryptocurrencies.
- Cybersecurity Incident Response Teams for Global Cyberattacks.

[7] The previous legislation:https://www.legislation.gov.uk/eur/2016/794/chapter/IV and the current legislation: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0991#d1e2253-1-1 could be found here.

1.2.4.1.8. PPP: Principles

The nature of cooperation is as varied as the types of private companies, non-governmental organisations (NGOs), academia and research institutes. The legal framework applicable to Europol provides for checks and balances to ensure that cooperation with private entities complies with principles such as:

- Conflict of interest.
- Respect for fundamental rights, in close connection with the rule of law.
- Compliance with the rules on confidentiality and exchange of information.
- Independence and impartiality.
- Transparency and accountability.

Level playing field in procurement and grants, as well as reporting and supervision. In instances where cooperation proves crucial, a concrete case arises in the analysis of Telegram communications, where the server relocates to a non-European country every six months, rendering the entire e-evidence acquisition chain an insurmountable challenge. Collaboration with third parties and Internet Service Providers (ISPs) becomes imperative to curb the continuous evasion of judicial and legal processes. Europol, equipped with a unit dedicated to immigration and human trafficking, approaches trafficking through a lens focused on the vulnerability of victims. Despite stability in percentages and the countries involved, a shift is noted with the emergence of Latin American and Asian criminal groups operating within European territories.
In recent years, a decrease in Nigerians in landing territories is observed, though prostitution and sexual exploitation persist, posing challenges for police forces and private entities engaged in analysis and prevention activities. European funds, available for investigators directly subsidized by the EU, can be accessed through Europol, offering support in various forms, including interpreters and technical activities.

1.2.3.5. Europol

Europol, functioning as a secure information exchange hub for law enforcement, faces underreported data challenges. The internet plays a crucial role in victim analysis and profiling. Police activities are becoming increasingly intricate due to the involvement of new actors such as online sexual services and novel payment forms offered by platforms. The emergence of crime-as-a-service on online

platforms highlights specific activities made available to organizations lacking skills, fostering collaborations with IT experts.

Forensic phone extraction has become more complex, adding weight to investigators' tasks. To align the criminal world and the realm of justice, directives like the E-evidence Directive, the Budapest Convention, and legislative interventions are in place. Europol collaborates with ISPs to request social profile closures, while the Innovation Lab, a working group, facilitates the exchange of best practices among Police Forces. It serves as a common repository for information on acquiring data from ISPs, providing contacts and methodologies. Dedicated to criminal investigations of cyber pornography and internet use, the Cybercrime Center within Europol acts as a promoter of investigative activities, collecting information from private entities that requires acquisition through national structures.

1.2.5. VICTIMS AND TRAFFICKING: THE EXPERIENCE OF THE THIRD SECTOR

1.2.5.1. National Anti-Trafficking Network

1.2.5.1.1 Standard Operating Procedures

There are separate measures to ensure adequate assistance to victims of trafficking and/or victims of serious exploitation such as:

- Identification
- First assistance and protection
- Long-term care and social inclusion
- Assisted voluntary return and social inclusion
- Access to justice.

The new National Referral Mechanism (MNR) for victims of trafficking* (October 2023) aims to:

- Provide a useful support tool to contribute to the correct and early identification of victims of trafficking in human beings and/or serious exploitation.
- Promote a multi-sectoral and multi-agency approach among all actors involved during the different stages needed in the fight against trafficking and serious exploitation, in line with existing human rights protection standards.

- Strengthen coordination and collaboration between public and private social bodies.

The activity of collaboration with the Public Prosecutors, from 2000 to the present, mainly develops on two axes:

- Accompaniment to the complaint of the victim of trafficking.
- Reception of victims of trafficking that emerged during the investigation.

In this time frame, the types of cases detected are distributed as follows:

- 95 %of sexual exploitation (on the street, indoors as e.g. Chinese massage salon).
- 5 % of forced begging.
- They are placed in contexts in which it is essential to issue a residence permit under Article 18 of the T.U.I. 286/98.

Joint training courses were useful for law enforcement, including:

- TAMPEP seminar (June 2002): training course for staff of international NGOs, medical personnel, and police officers, present in Albanian territory. Objective: export of the model to fight the Italian trade sponsored by UNICEF and IPH-RAR Focal Point in Vlora, Albania.
- TAMPEP seminar (October 2002): training course on Article 18 TU 286/98 for government staff of the new Anti-Trafficking Committee of the Republic of Croatia. Objective: create a network between actors of anti-trafficking activities in Italy and Croatia.
- European Network against Trafficking (JLS/2006/AGIS/169), continuing under the AGIS 2004 Programme (JLS/2006/AGIS/169). Objective: strengthen and promote cooperation between magistrates and law enforcement agencies operating in the field of combating trafficking for the purpose of sexual exploitation, and public and private bodies of assistance to victims and protection of rights.

1.2.5.1.2. New Challanges

The phenomenon of trafficking in human beings and serious exploitation in recent years has become increasingly complex, changing in terms of:

- Victims involved (increase in men, transgender people, MSNAs and mothers with children).

- New areas and methods of exploitation (increased cases of severe labour exploitation, multiple exploitation, and new contexts).
- New Countries of Origin of Persons Victims of Sexual Exploitation.
- New recruitment methods: through new digital modes, such as social networks and other applications.
- Takes place in its own country of origin, in the countries of transit.
- Particularly vulnerable people already present in Italy, especially in the workplace, are at risk of serious exploitation.

1.2.5.1.3. Emergence and Taking Charge: Key Elements

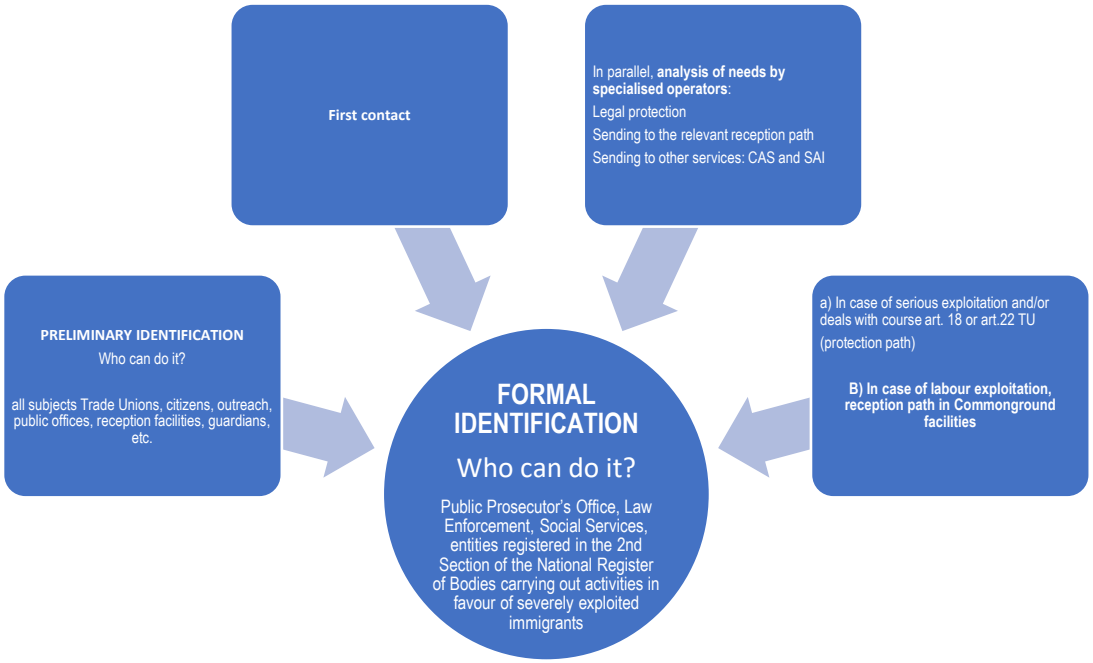


Figure 5: Key Elements in Emergence

1.2.5.1.4. Critical issues in the last year

- The main problems recorded in the last year of activity include:
- Arrival flow of migrants from the Balkan route – more than 12 thousand since the beginning of 2023.
- Numerous reports of potential victims of trafficking and vulnerable persons, exposed to violence and conditions of severe exploitation along the routes (only women, young women, MSNA, young men).
- Need to carry out rapid interventions for the identification of elements of trafficking especially for those who are transiting even in a multi-agency perspective.
- Lack of shelters, especially for women and families.

- Non-distribution of resources allocated to anti-trafficking bodies.

1.2.5.1.5 Equality Social Cooperative

The NAVIGARE project assigns the responsibility for emergency response and assessment activities to the Equality Social Cooperative team. At the core of their discussions lies the profound impact of online trafficking, which has reshaped paradigms by introducing novel communicative codes, effectively obscuring the phenomenon, and rendering victims practically invisible. The recruitment process, especially targeting young underage individuals with limited cultural backgrounds, predominantly takes place on social media, leveraging the guise of sentimental relationships to establish a deeply rooted trust that proves challenging to dismantle. Among those vulnerable to exploitation are unaccompanied minors, including a significant number of Tunisians, often caught in the dual role of both perpetrators in drug dealing and victims of exploitation crimes.
The online network serves as a tool for tracking, control, and intimidation tactics, including the filming of victims during sexual acts for potential public exposure. Labour exploitation employs geolocation technologies, utilizing apps or electronic bracelets for monitoring. Victim support organizations are adapting to digital landscapes, creating virtual platforms and spaces to aid in emergence and offer assistance. The introduction of a virtual operator application serves the urgent need for immediate help and continuous support.

The critical necessity for digital literacy, particularly in comprehending the intricacies of illegal activities, underscores the demand for a multi-agency response. Such collaboration is essential in addressing this issue across different stages, aiming not only to prevent victimization but also to foster collaborative global solutions.

1.2.6. PUBLIC-PRIVATE COOPERATION IN DEALING WITH CASES OF HUMAN SMUGGLING AND TRAFFICKING IN HUMAN BEINGS: THE EXPERIENCE OF THE PUBLIC MINISTRY

Public-private collaboration constitutes a reciprocal exchange built on mutual trust and knowledge. The private sector contributes valuable information, while the public sector, particularly judicial authorities, provides legal outcomes. The vital role of victim support organizations cannot be overstated, offering

alternatives, assistance, and pertinent information crucial for investigations. Without their support, apprehending individuals would merely address one aspect, leaving them ensnared in the same phenomenon.

This underscores the significance of establishing relationships and connections with trusted individuals in the field, adopting a tangible and hands-on approach that includes thorough analysis of all interceptions. Modern models of infiltration have evolved, emphasizing the increasing importance of the internet as it operates through channels that lack physical presence. The role of infiltration activity has consequently transformed. Understanding the evolution of trafficking from the Balkans considering these changes becomes a challenging endeavour.

1.3 Quotes / Significant Statements / Recommendations:

Former Prosecutor

- Europol's role seems to be limited in comparison to the significance of the protected legal assets, whereas it should elevate the Regulation to a lex perfecta by enforcing the compulsory removal of content, rather than remaining a *lex minus quam perfecta*.
- The Regulation holds immense potential for combating various serious illegal activities conducted through the internet, extending beyond terrorism, and could effectively broaden its scope to address these issues.

Prosecutor

- Human trafficking is propelled by small yet well-organized organizations, making it imperative to comprehend their modus operandi. Accordingly, prioritizing the specialization of the Judicial Police is crucial.
- The second priority lies in fostering collaboration between Public Prosecutors and significant internet entities. Understanding the dynamics of this interaction, identifying the involved parties, and discerning the financial aspects are essential. Law enforcement agencies lack sufficient resources to compensate internet analysts. Nevertheless, there is optimism as technology can significantly aid investigations.

Intel Analyst

- Human trafficking is a criminal activity that has always been able to adapt and evolve quickly. This is also true with the advent of the digital society.

- The impact of the Internet and new technologies on crime and deviant behavior is pervasive and multi-faceted.
- One of the most important roles played by the Internet is facilitating the so-called "lover boy method".
- Even if social media is probably the most important virtual channel, other digital environments and platforms are also particularly suitable for the facilitation of the lover-boy method.
- The responsible parties make sure that the victims feel secure and implement the necessary security measures to prevent retaliation, re-victimisation, and re-traumatisation.
- Importance of the end-to-end and holistic approach.

Representative of ISP

- Since 2017, it is possible to identify and remove content even without waiting for orders from an administrative or judicial authority.
- The winning model is the cooperation between public bodies, in charge of law enforcement and connoisseurs of illicit phenomena, and the subjects "Private", providers of digital services misused for illicit purposes.

Deputy Prosecutor

- Significance of cash flow analysis, particularly in money transfers.
- Investigations into trafficking inherently encompass international elements, necessitating the essential use of international judicial cooperation instruments.
- Social networks play a crucial role in both the recruitment and sorting phases of the trafficking process.
- Recognition of the public-private partnership as a connecting link.
- Public-private collaboration facilitates a reciprocal exchange where each party contributes based on their available expertise.
- Support from victim support organizations is indispensable.
- Ongoing development of new models for infiltrators.

Judge Preliminary Investigations

- New interpretative guidelines.
- Judicial cooperation also with countries with which it was unimaginable a short time ago.
- Valued importance of technological testing.
- Process "around the victim" instead of "upon the victim".

Europol

- Cooperation between law enforcement and the private sector is crucial in the fight against trafficking in human beings.
- The legal framework applicable to Europol provides for checks and balances to ensure that cooperation with private entities complies with certain principles.
- European funds are available for investigators directly funded by the EU, including through Europol.
- The role of the internet today is crucial for the analysis and profiling of victims.
- Police activity is increasingly complex due to the intervention of new actors.

NGO Victim Protection

- Creation of a new national referral mechanism for victims of trafficking.
- Collaboration with the prosecutors.
- Importance of joint training courses and multi-agency approach.
- The phenomenon is taking on increasingly complex connotations, changing under different profiles, especially the online dimension that is changing all the paradigms known because it uses completely different communicative codes.
- The "lover boy" technique.
- Call for opportunities in digital, for the adaptation of the legislation of NGOs dealing with victims of trafficking and urgency to receive instructions on the digital dimension.
- Need for a multi-agency response involving actors from the different phases of the phenomenon.

1.4 Needs and Challenges:

1 Europol's role of mere coordination and surveillance appears to be reductive in relation to the importance of the legal assets covered by protection, when, instead, more appropriately, it should be of an enforceable nature, thus making the Regulation, through the compulsory removal of contents, lex perfecta.

2 The Regulation introduced by the European Parliament and the Council has an enormous potential to combat other serious illegal conduct perpetrated through the web, such as those in the field of combating illicit

drug trafficking, child pornography and gender-based hate crimes and racial discrimination, which could well be included in its scope. It could be the European Commission to extend the scope of this order also to other contents and according to prevention.

3 What is necessary for effective public-private cooperation? The INTERCEPTED project aims to create a model that broadly retraces the topic of Removal Regulation with an experimentation of extension of the model in a field other than terrorism. Experimentally it is based on a voluntary alliance intelligence, i.e. a voluntary link between these stakeholders together with the competent authorities for the prevention and repression of crimes applied to the trafficking sector, in order to transform what may appear as a slogan into a structured and organised element.

4 The Project will allow to equip itself with OSINT platforms that will allow to reconstruct many elements related to those involved in the trafficking through social media, chat, geolocations, deep web, always within the framework of GDPR tools. The private sector can collect these materials by managing them with forensic techniques, i.e. they also have probative value.

5 Experimentation of new models in which private individuals would face the problem at an earlier stage, when it does not yet have procedural or investigative value (pre-investigative) using research tools that generate useful content both for the judicial authorities but also for the analysis of trends and geopolitical situations.

6 The digital transition requires different models: digital HUMINT is one of them.

7 Problem of the unevenness of the regulatory framework at European level.

8 The funds can be obtained by submitting project proposals to Europol and the European Commission.

9 The transition on the internet has become very important because it is organised on channels that do not move physically, and therefore the infiltration is completely different. For this reason, it is not easy to understand how, for example, the route has evolved from the Balkans.

2. GREECE

2.1 Brief Description of FG Organisation:

On Tuesday 21st of November 2023, KEMEA delivered the aforementioned focus group titled: "Online Trafficking: Trends, Challenges, Needs". The focus group meeting took place online, on Teams platform, due to participants' availability. In total, 8 first-line practitioners attended this meeting, led by KEMEA's team. More specifically, the meeting was attended by:

- 3 Police Officers
- 1 Public Prosecutor
- 2 Representatives from the Hellenic Telecommunications & Post Commission (EETT)
- 2 Representatives from the NGO "The Smile of the Child"
- 3 members of KEMEA's team

The focus group meeting commenced with a tour de table to get to know each other, followed by a presentation of INTERCEPTED project (objectives, outcomes, results, KEMEA's role). Then, the discussion focused on three main subject areas, according to the agenda:

- "Existing trends in the recruitment of victims of Human Trafficking".
- "Challenges, needs, gaps in fighting Online Trafficking".
- The role of Internet and the usage of social media in the recruitment of victims of Online Trafficking".

The meeting lasted for 3 consecutive hours (without break).

2.2 Relevant Inputs, Key Results and Findings:

Public Prosecutor input:

- Many EU countries (such as: Belgium, Croatia, Netherlands, Greece, France) have been convicted by the European Court of Human Rights on the labour area for not reassuring/protecting the right of freedom from forced labour.

- The main alluring tactic for recruitment of victims happens online, with the use of technology. Thus, fraud is the main tactic used by the perpetrator/purchaser to approach the possible victim.

- Due to the transborder dimension of the phenomenon of online trafficking, there are many issues arisen on the evidence collection. More specifically, the difficulty lays on the fact that evidence is collected in a different country than the country where the evidence will be used in court. Thus, it is likely that the way with which the evidence has been collected in a X country may not apply in Z country, favouring perpetrator's/purchaser's impunity.

- Many trafficking cases that are examined by the Public Prosecutor contain vague and unclear information, resulting in inability to process those cases. However, Public Prosecutor doesn't reject the above cases, instead they ask for supplementary evidence to set the cases, addressing to the private sector for their support.

Hellenic Telecommunications & Post Commission (EETT) input:

- In Greece, regarding the online content, EETT is only responsible for disrupting an online content after a wit being issued. They are not responsible for investigating illegal content online.

- To their opinion, ISPs can't be responsible for investigating inappropriate and illegal content online. This is out of their scope, and they don't even have the know-how to do so. Of course, they are in cooperation with the authorities to provide requested information, for instance who is behind a certain IP.

Hellenic Police input:

- To combat human trafficking, Ministry of Citizen Protection has established 2 Anti-Trafficking Units within the General Police Directorate of State Security in Athens and Thessaloniki.

- Regarding the advertisement of trafficked services, it is difficult for LEAs to identify the purchaser/perpetrator, as they make use of online platforms to recruit their victims, offering them anonymity. Those online marketplaces facilitate online traffickers, making really challenging to be investigated and arrested.

- Vulnerable groups mainly targeted for purposes of exploitation are women of low income, women with no protective parental environment, women coming from an abusive environment, men of lower income being victims of labour exploitation.

- During the last years, in Greece, it is very common the use of WhatsApp groups titled "Find a job in Greece", without specifying the kind of job, to recruit possible victims.

- In Greece, the tactic of "lover boy" does exist, with the perpetrator usually being close to the victim.

- Nowadays, THB victims are not subjected to physical violence. They do subject, though, to psychological and emotional abuse. This is why in many cases the victims do not consider themselves as victims, as they have in their mind that the victimization is only linked with physical abuse.

- Regarding the information exchange on THB cases, Hellenic Police is working closely with the contact points of INTERPOL, EUROPOL and SIRENE.

- Online platforms mainly used for exploitation purposes: WhatsApp, snapchat, TikTok.

<u>The smile of Child input:</u>

- It is difficult to collect data on human trafficking victims, as it demands a legal process to characterize a person as "victim of human trafficking".
- Most cases that reach to us are related with aiding and sexual exploitation of minor girls.

- The victims are coming in contact with us using our hotline 1056.

2.3 Quotes / Significant Statements / Recommendations:

Prosecutor:

- "When a THB case is adjudicated, it is highly recommended to collect and pay attention to indirect evidence. Specifically, in cases of organized criminal groups, it is very difficult for the victim to accuse its perpetrator. This is why in such cases, it is very likely the victim to have been turned into perpetrator to reassure better life conditions for itself".

- "In THB cases, it is very important to follow the money, as they are related to money laundering activities".

- "As THB is a transnational, complicated and multi-crime related phenomenon, the cooperation between public and private sector could bring positive and effective results against the THB fight".

EETT:

- "In Greece, only the Public Prosecutor is responsible to consider online content as inappropriate or/and illegal. There is not, so far, a competent authority authorized to identify illegal content online. Thus, it is very crucial the establishment of a public authority responsible for checking/auditing/monitoring the content disseminated in online platforms".

- "Illegal or/and alluring content spotted in social media platforms could be reported by legal bodies (not citizens) in the EU Single Market for Digital Services (DSA) by February 2024, where this mechanism will be put in place. In that way, the responsible ISP will be obliged to remove the inappropriate content".

Hellenic Police:

- "The proper exchange of information among the relevant stakeholders can be very helpful and effective for the investigation of a THB incident".

- Greek hotlines for reporting THB incidents: 100 (Hellenic Police) & 1109 (NGO A21).

- "The technological tools could contribute and support our work in the primary prevention of THB".

2.4 Needs and Challenges:

1 In Greece, there are not existing protocols or standard operating procedures (SOP) for the competent authorities to follow in cases of THB. The competent authorities involved (Hellenic Police, Judicial Authorities, NGOs) have set a mode of cooperation among them in terms of information exchange to handle THB incidents. However, it is mandatory to put in place mechanisms and procedures in order to enhance inter-agency cooperation among the relevant stakeholders for an effective response to THB phenomenon. Under that framework, it is essential to set clear responsibilities of the competent authorities and clarify the level and the extent of their involvement, as it is observed that there is overlapping of responsibilities.

2 The competent authorities should receive proper training on how to identify and handle THB incidents.

3 In Greece, the time of investigation for THB incidents should be limited, being effective and complete at the same time.

4 Although Hellenic Police has an established communication with INTERPOL, EUROPOL and SIRENE, in many cases, third countries (where responsible) pose difficulties in information sharing.

5 Even the existing legal framework on THB issues is sufficient, it is challenging how we could "force" competent authorities from other countries to share the relevant information with the Greek competent authorities.

6 The Greek legal framework could be tightened up regarding the suspensive effect of sentences for committing crimes related to online trafficking.

7 Alternative forms of sentences, e.g., utility work, could be inserted into the existing legal framework for committing such crimes.

8 Within the social media content, it is often hard to collect appropriate information. Many of those social media platforms offer the possibility to share messages, photos, and videos and after being sent and therefore being seen only once by the user to immediately disappear.

3. SPAIN

3.1 Brief Description of FG Organisation:

The Focus group was organised in the venues of the Euro-Arab Foundation for Higher Studies (FUNDEA), in Granada, Spain on 30 November 2023. Participants could also join online.
Jose M González Riera led the FG. Additionally, Josaima Peregrina took notes. Both are researchers at the Euro-Arab Foundation.
The focus group lasted for three hours, from 4:00 to 7:00 pm.

Participants:

- Francisco J. Hernández Guerrero. Delegated Prosecutor of Cybercrime of the Public Prosecutor's Office of Granada.

- Ana Isabel Cruz Ortiz. Director of the Center for Minors 'ISL La Huerta', Granada.

- Habiba Hadjab Boudiaf. Intercultural Mediator of the Service of Protection of Minors of Granada.

- Ainhoa Rodríguez García de Cortázar. Technician in Childhood. Sociologist. Member of the Childhood Observatory.

- Alexandra Toma Simeoni. Legal advisor of the Delegation of Loja (Granada) of Mujeres en Zona de Conflicto (Women in Conflict Zone, MZC).

- Pablo M. Melgarejo Cordón. Professor of the Department of Private International Law. University of Granada. Expert in online trafficking.

Even though eight participants confirmed their participation, two participants could not finally join:

- Susana Garcia-Baquero Borrell. Public Prosecutor of Trafficking in Vigo (Galicia, Spain) could not access to the videoconference connection due to technical issues.

- Jose Ignacio Sanchez Lopez. Head of the Alien and Border Brigade. National Police, Granada, finally had unexpected professional duties that he had to attend urgently.

3.2 Relevant Inputs, Key Results and Findings:

3.2.1 VICTIMS' PROFILE, EXPLOITATION & RECRUITMENT

3.2.1.1. Post-Covid Trends

As far as minors are concerned, the latest UN report confirms that the tendency to sexually exploited girls has increased. After Covid-19, the trafficking market has diversified and is expanding. There has been an increase in other forms of exploitation, beyond labour, where we see an upsurge in exploitation of boys. There is also another emerging type of trafficking: illicit, criminalised activities.

Among the most vulnerable groups, it is worth highlighting all the people in fragile situations (displaced people, re-settled people...), "people who's right to live has been taken away". It is also worth mentioning people with mental health problems, special needs, the LGTBI collective. In addition to migrant trafficking, there are also national victims. A few months ago, there was a case of trafficking of Spanish teenagers who used online photos in Almendralejo (Badajoz, Spain).

3.2.1.2. Modus Operandi

Research and investigation have become obsolete, as during this post-pandemic period, criminal organisations have changed their procedures. In other words, almost all activities are mainly carried out digitally. Through the Deep Web and the Dark Web, via highly sophisticated platforms capable of moving huge amounts of money. *"While we are discussing on how to define the legal contours of online trafficking, criminal organisations have already moved further ahead."*

We are detecting in various sectors what is called CAS, "crime as a service". There is not really a single criminal organisation that develops all the phases of an illicit market, a criminal market, such as, for example, human trafficking. What does exist is a command-and-control nucleus, which oversees the direction of the whole project, which is renting or carrying out collaboration with other criminal groups. This projection, this economic benefit and how it is developed in the market, effectively takes place online, it is carried out in the cryptocurrency markets and is a way of hindering traceability, of laundering the money.

However, the same criminal group that is carrying out the trafficking activity does not do this. A group that is dedicated to this and that provides its services for hire to a trafficking organisation is doing it. The elaboration of those messages of those platforms or those recruitment pages can be developed by people or groups that are specifically dedicated to that function that are rented by the main group.

Recruitment is implemented by a specific group of people who are hired for this purpose. It follows the law of the market. They are temporary joint venture, which represents a major difficulty to tackle. You only get to the intermediate steps (The one who controls the house where the girls are, etc...) Going up these levels means advancing in technological equipment. This challenge must be assumed by police structures and authorities that move away from citizen security and towards national security. The approach must be hybrid: including criminal investigation and national security investigation.

3.2.1.3 Detection

These organisations need many virtual connections, they use massive digital platforms and that offers many opportunities to detect them, but we need to know what to look for. These digital connections represent opportunities for traceability.

3.2.2. Protocols and Tools

Question: What specific protocols are in place to combat online trafficking?

General lack of protocols, training, resources, and tools

In general, there are no specific protocols for detecting and reporting this recruitment as victims of online trafficking in shelters and services for women victims of sexual exploitation. There is a lack of resources, tools, and training.

Future MZC protocol

Women in Conflict Zone workers are developing a protocol to detect and report online trafficking.

Welcome protocol of the Minors' Services in Grenada

That said, the Granada Minor Service (Servicio de Menores) considers the mobile phone to be the point of contact with the criminal agency, so it has a specific internal protocol: when a minor arrives who shows signs of being a victim of

trafficking, her mobile phone is taken away as part of a comprehensive welcome protocol. Experience has shown that, since 2008, in Granada, all the girls who have been admitted to child protection centres and who have had access to their mobile phones have run away almost the next day.

Notification to the authorities: indicators of trafficking

The Child Protection Service of Granada has a contact, through an internal protocol. When they detect minors using certain networks, for example, OnlyFans, Instagram, Twitter, or any other social network, they notify the authorities. However, it is not because they use a social network that they are potentially victims; The Child Protection Service counts with indicators of trafficking, which, if they are activated, are reported to the National Police so that they can intervene in case there is a real danger.

Requirements for developing a protocol for detecting and reporting trafficking online

In terms of establishing a detection protocol, the development of a database containing information about trafficking victims is essential. This database can be created provided we have the necessary means and resources. The information for this database would be sourced from the fields and variables already present in the definition of trafficking itself. With details on actions, means, and ends, a comprehensive list of indicators can be compiled, forming the basis for both a database and a potential application. Additionally, valuable information from the victims' phones could serve as an initial point of reference.
For cases involving minors, obtaining authorization is imperative, and the judge must approve the data extraction. The protocol should encompass the following key elements:

1. Professionals should be able to indicate potential trafficking indicators.
2. Information from the phones must be extracted.
3. Academia should comprehend the patterns.

Subsequently, collaborative efforts involving various stakeholders, including law enforcement, authorities, and the police, are crucial for effective prosecution. This necessitates the establishment of a protocol defining joint participation by the Ministry of the Interior, the General Council of the Judiciary, and the Public Prosecutor's Office. Similar collaborative protocols, such as those in place for hate crimes and other relevant matters, can serve as models for this endeavour.

The necessity of replicating the tools employed by trafficking networks

These criminal organizations, governed on a multinational scale, utilize robust digital platforms to exploit victims. It is imperative to emulate these criminal entities and combat them using analogous means, as "networks are fought with networks." Their effectiveness thrives on our disorganization, despite possessing adequate resources. Therefore, there is a need to organize information, identify victims, extract their data to recognize patterns, and integrate Artificial Intelligence to systematize the acquired information.

Trafficking networks as a national security problem: victims as weapons of war

"We are investigating networks that are almost equivalent to terrorist organisations, and this has to be done with an intelligence, national security mentality. Because some of the victims are also victims of war, which means we have another conflict. The fact is that many of our victims, especially sub-Saharan victims, are used as migrant weapons [...] that are used to blackmail or even to advance on Europe".

Use of AI

The efficacy of artificial intelligence in combating trafficking is questioned due to the handling of sensitive data such as foreign nationality, race, national origin, or gender.

Use of the digital undercover agent as a tool for detecting trafficking

While undercover agents in the Anglo-Saxon world prove effective, in Spain, their use may be construed as incitement to crime. This poses challenges and potential issues, requiring meticulous preservation of evidence with a chain of custody and adherence to specific presentation protocols. Though complex as evidence, the Judicial Police of the Guardia Civil and the National Police employ them in their investigations.

The digital undercover agent can be instrumental in infiltrating a person into the criminal organization, such as working as a recruiter. Alternatively, AI could be employed to impersonate created individuals offering such services online.

The digital undercover agent can be instrumental in infiltrating a person into the criminal organization, such as working as a recruiter. Alternatively, AI could be employed to impersonate created individuals offering such services online.

3.2.2 LEGAL FRAMEWORK AND RESPONSIBILITY OF SOCIAL NETWORKS

A Legal framework without a national plan

Despite the existence of a legal framework on social networks, there is not a unified criminal policy against THB in Spain. Unlike the Spanish National Plan on Drugs or the National Plan against Hate Crimes, there is no national plan against THB, where the State defines and establishes the forms of cooperation between all the administrations and begins to provide training and resources. Those two plans establish protocols for police units to ask certain questions when faced with victims. The future THB plan should also institute indicators of trafficking that are activated because trafficking is going to have national security connotations.

Anti-Trafficking Bill

The draft of the anti-trafficking bill was presented in November 2022. While this legislation is commendable, there are numerous loopholes in its application. Currently, a minor migrant in a child protection center cannot be identified as a trafficking victim based on the interpretation that, as a minor under guardianship, they already have protection. In this context, victim services emphasize that if there are indicators of trafficking, the minor should be identified as a victim of THB as per the definition established by regulations. It's not just a matter of offering institutional protection to the child but also ensuring their safety. The fact that they are in a center for minors doesn't preclude them from accessing platforms like OnlyFans or having contact with their traffickers.

Legal regulation of the use of AI for victim impersonation

Within existing legal mechanisms, artificial intelligence theoretically cannot be used for victim impersonation presently. However, in five years' time, using the victim's mobile phone, AI could impersonate the victim with a bot to interact with the criminal trafficking organization. This digital bot would have learned the victims' speech patterns, eliminating the need for an undercover agent, and minimizing risk to the victim. In the future, we will need to authorize the use of such chat interactions to avoid procedural problems.

"The databases used in the Ministry of Justice are subject to data protection and the presumption of innocence. Therefore, you cannot give the AI biased data, unless you have a justification for using sensitive data. Everything we are going to use here in trafficking is sensitive data. It's minors, it is women, it is sex life, its sexual orientation, it's racial. In other words, we are dealing with the most sensitive aspects in our society. But we will be avoiding the problem of victimisation, we will

be able to maintain contact with the criminal organisation and we will not have the procedural problems".

Type of revision of the legal framework that AI would entail.

Both the regulations governing artificial intelligence and procedural laws themselves must establish new investigative measures, allowing, for instance, the creation of virtual images of an individual. This is a significant development, as it involves depicting an offender in a digital format. Article 85 of the proposed Artificial Intelligence Regulation stipulates that, as human beings, when dealing with artificial intelligence, we must be aware that we are interacting with an artificial intelligence unless it's during a criminal investigation.

3.2.3. RESPONSIBILITY OF SOCIAL NETWORKS

Digital Services Directive

The Digital Services Directive (2022) outlines the obligations for digital service providers concerning child protection. In essence, it establishes a basic regulatory framework encouraging servers to collaborate, akin to a new social contract the European Union is forming with the platforms.

THB-related content should be mandated for inclusion, necessitating obligatory collaboration with authorities. This entails prompt removal upon receipt of a complaint, a practice already observed in Spain for hate content, which the Attorney General's Office commits to removing within 24 hours. Additionally, immediate collaboration in sharing information to facilitate THB prosecution is crucial. The European Union might consider expanding and updating the content for which digital platforms are obliged to collaborate with EU states, particularly content related to human trafficking.

Rather than compelling Internet Service Providers (ISPs) to enhance collaboration, it is crucial that they recognize the inclusion of this content within their existing obligations to collaborate.

Dysfunctions in content removal

MZC has noticed that some websites are shut down, but then they will be recreated under another name, even though it is the same groups that run it. This is the case of ads on Facebook that are fake massage job offers.

3.2.4. COOPERATION

The need for a multidisciplinary approach

"We lack a multidisciplinary and organic approach. It is necessary to form working teams within the administrations themselves, LEAs, for example, and judicial and prosecutorial authorities. They would cooperate both for specific cases and for the evaluation of these policies, to see how they work effectively over time."

Regarding interdisciplinary cooperation, it is already reflected in the regulations in the case of minors. The Public Prosecutor's Office is supposed to convene an interdisciplinary meeting every six months between professionals involved in combating child trafficking, as established in the 2014 Framework Protocol on migrant minors. However, as it is a recommendation and not a mandatory rule, such a meeting is not held in any of the eight Andalusian provinces, except in Granada. This meeting should be mandatory.

Other cooperation protocols

There exists a national protocol on trafficking that requires linkage to each autonomous community, but its implementation at the regional level is weak. Andalusia is developing a specific protocol for minors victimized by trafficking.
Addressing Challenges in Implementing Cooperation Protocols Participants emphasize the need for a national plan of action on trafficking, coordinating all administrations, roles, and instruments.

How would you address the challenges in the implementation of a cooperation protocol for the provision of information on recruitment and advertising of trafficking?

Participants reiterated the need to establish a national plan of action on trafficking, where all administrations, roles, and instruments to be used are coordinated.

European cooperation

At the European level, collaboration occurs in concrete operations and specific investigations through EUROJUSTICE. Moreover, at the criminal intelligence level, cooperation takes place within the police agency, a dedicated criminal intelligence unit. This unit conducts strategic and operational analyses of specific sectors and engages in collaborative efforts for specific investigations. However, at the level of the Public Prosecutor's Office, there is no forum or organization at the EU level. In Latin America, for instance, there is the International Association of Public Prosecutors, fostering extensive contact and specific networks.

The challenge arises from differences in legal cultures among the 27 EU countries. Currently, there is an issue with the investigative measures that can be adopted. For instance, in the interception of communications or cross chat, France allows prosecutors to authorize the police to use a Trojan horse, but this is not the case in Germany or Spain.

Establishing cooperation among prosecutors, as seen in Latin America, would be beneficial. Encouraging an exchange of best practices within the EU is also advisable. Nevertheless, police units in Europe play a more prominent role and collaborate more extensively.

National cooperation

At the national level, within the Public Prosecutor's Office and its specialized networks, an Aliens Unit operates with a Coordinating Prosecutor appointed by the Attorney General of the State. Additionally, there are two deputy prosecutors and a liaison officer, one from the National Police and another from the Civil Guard. This structure is present in all units. Consequently, prosecutors can approach the police to request information. Coordination is established at the national level through the State Attorney General's Office, transmitting it to the attorneys' action networks. They establish uniform criteria to maintain the unity of action within the Public Prosecutor's Office.

3.2.5. TRAINING

Training to combat trafficking online

Victim protection and child protection services point out that there is a lack of training in detecting victims of trafficking, but online is even more specific and they do not receive any such training. They feel they could collaborate in the online recruitment phase. They work with the victims, but in order to detect those victims, we need to see what indicators are the factors that constitute the crime. Usually, it is these same organisations that offer training to each other, in the absence of training offered by the public authorities.

3.2.6. RELATIONSHIP OF TRAFFICKING WITH OTHER CRIMES

How does trafficking interrelate with other crimes?

Trafficking relates to many crimes, perhaps it would be interesting to look closely at tax evasion crimes, which may be the key. This requires coordination of partners from various sectors.

How does online trafficking intersect with offline trafficking?
"Everything digital leaves traces, which allows us to know more things, we need to have the equipment to track and the regulatory instruments to combat it. My impression is that the prosecution against human trafficking is happening in the natural world, but not in the digital world."

3.3 Quotes / Significant Statements / Recommendations:

THB digital activities offer prima facie for detection and prosecution
[THB] “Digital connections represent opportunities for traceability”.

Gap between criminal investigation and THB organised crime
"While we are discussing on how to define the legal contours of online trafficking, criminal organisations have already moved further ahead."

Lack of expertise in cybercrime in the Police Aliens Section
"The Aliens Section of the [National] Police has no expertise in cybercrime because this is handled by the technological crime group, and they do not collaborate with each other. There is no training or awareness of multidisciplinary work, neither in the police, nor in the courts, nor in the prosecutors' offices. So, although they have the resources, as they are not connected, and perhaps they are in adjoining offices, they are not used".

Recommendation: use hate crime policy as an example
"In the area of hate and hate policies, when this has become a policy, a line of criminal policy, the [Spanish] State has taken it upon itself to train its police officers, to create special units and other media networks. All police units have their own protocols for dealing with hate. They know what they must do, they know what they must ask, what indicators they must take into consideration. Thus, through training and accreditation, [...] it can be achieved with the precedent of what has been done in hate policies".

Lack of protection for minors in the care of the Childcare Services

"We are talking about very vulnerable adolescents, with weakened emotional states who are cannon fodder to be recruited through a social network".

Internal protocol of the Granada Minors' Service

"The Granada Minors' Service has a specific internal protocol: when there is a minor who arrives with these characteristics, with these indicators of being a victim of trafficking, we take away her mobile phone within a welcome protocol. Because, if we don't remove the mobile phone, it's like staying in contact with the organisation".

Requirements for developing a protocol for detecting and reporting trafficking online

To formulate a detection protocol, we require a database, which resides on the mobile phones of the victims. The initial step involves obtaining their consent to access their networks and mobile devices, enabling us to identify relevant websites. In the case of minors, authorization is essential, and a judge must approve the data extraction.

A comprehensive protocol should include the following elements:

- Professionals should be able to specify indications of trafficking.
- Telephone information needs to be extracted.
- Academia must comprehend the patterns.

Subsequently, a collaborative effort involving actors, police, and authorities is vital for effective prosecution. Establishing joint participation requires a protocol coordinated by the Ministry of the Interior, the General Council of the Judiciary, and the Public Prosecutor's Office, like existing protocols for hate crimes and other matters.

"Databases do not exist for purchase; they must be developed with multiple functions. The primary source for this development is the field information present on the victims' phones."

The need to copy the tools of the trafficking networks

"To be able to access victims, traffickers need to have a super powerful digital platform. So maybe we should copy criminal organisations in order to maybe be able to vary, we should do the same."

"Networks are fought with networks. Networks work because we are disorganised, we have the resources, but we do not have organisation. We need to organise the information, we need to identify the victim and extract the data from them, which allows us to identify the patterns, dump the patterns, organise them and use even AI. But the perspective cannot be one of citizen security, but of national security".

Trafficking networks as a national security problem: victims as weapons of war
"We are investigating networks that are almost equivalent to terrorist organisations, and this has to be done with an intelligence, national security mentality. Because some of the victims are also victims of war, which means we have another conflict. The fact is that many of our victims, especially sub-Saharan victims, are used as migrant weapons [...] that are used to blackmail or even to advance on Europe".
"We are on the first ring: the victims, we need to go further. We need to go up steps. These are other parameters of investigation that move away from the traditional police investigation."

Use of Artificial Intelligence
"In AI in the [Spanish] State we are just starting [...] I would not be so optimistic about using artificial intelligence in this field, because we have several sensitive issues and sensitive data: foreigners, race, national origin, gender, and all of these generate a bias in the algorithms that is very dangerous. So artificial intelligence is not exactly, I think, nor is it going to be, a priority, not even as a research tool. However, we can fill in those patterns that we know with concrete data and see where the networks are.

Using the digital undercover agent as a tool for detecting trafficking
"It is a big problem in its essence. Its use has to be done with a lot of safeguards, the evidence has to be preserved with a chain of custody, then it has to be presented in a certain form."
"The digital undercover agent can be used when you are going to introduce a person into the criminal organisation, as part of it. Therefore, for example, you are going to make him work as a recruiter in such and such a place. That would be the job of the undercover agent. As a digital undercover agent, we [public prosecutors] have a lot of doubts about the use of undercover agents when, for example, you are going to pose as a victim. That's why we don't like it, because very relevant investigations make use of a start that may be weak. And it is also not necessary. It is more important to detect where the search patterns are, because, for example, maybe the recruitment messages are either on a platform, basically, or in a

Telegram group" [...] But in any case, we must use it very carefully because we are on the borderline with provoked crime, at least in Spain, and then, how do we prove all this with evidence?"

A legal framework without a national plan

"We have plenty [regulations]. What we don't have is a unified criminal policy. So, just as, for example, the issue of hatred suddenly exploded and a national action plan or a national drugs plan was established. [However] there is no national plan against THB, where the State delimits and establishes. Where the state comes together with the administrations that have something to do with it and establishes the obligatory forms of cooperation between them and begins to provide training and resources. Why? Because people are being exploited and because it is going to have national security connotations [...] And that requires the State to really get its act together and establish all the measures at all levels, each one in its own field".

Future legal framework for AI

"The databases used in the Ministry of Justice are subject to data protection and presumption of innocence. So, you can't give the AI biased data, unless you have a justification for using sensitive data. Everything we are going to use here in trafficking is sensitive data. It's minors, its women, it's sex life, it's sexual orientation, it's racial. In other words, we are dealing with the most sensitive in society. But we are avoiding the problem of victimization, we are being able to maintain contact with the organization and we don't have the procedural problems."

"In about five years, artificial intelligence can be used to replace the victim. Artificial intelligence in Justice and Police does not yet work, and there is still a lot of legal development to be done. However, for example, if you have detected that a minor victim, in contact with his phone through chats with the organization, not only maintains contact, but also can flee. Artificial intelligences can replace the victim by learning how he has spoken from the content of his phone, learning what his/her tone is, his words and can maintain contact for them. So, there is no need for an undercover agent. It is that we have a digital bot that can simulate based on that information, of course, of thousands of victims, how they speak and have a much more effective undercover agent. That is, for example, a use of artificial intelligence that replaces all of this and we don't have the problem of the minor, it's not affected, but we're replacing it. Moreover, we don't have a problem of a covert agent. We simply have to authorize the use of a digital assistant or a virtual undercover with an agent."

Type of revision of the legal framework that would involve AI

"Artificial intelligence tools, being disruptive technologies, pose more significant risks than the conventional IT tools we currently possess. This is primarily due to our limited understanding of how these intelligent systems will behave and handle the data they generate. At present, we are grappling with the challenges posed by generative artificial intelligences, specifically concerning legal implications. These systems generate language, images, or sound, and we are just beginning to address the associated issues.

For instance, the Proposal for a Regulation on Artificial Intelligence suggests a framework: "If you utilize a generative artificial intelligence that produces images resembling real individuals, you must inform and alert me about the use of artificial intelligence.' This obligation is explicitly outlined in Article 85 of the regulation. Therefore, we now have a guiding principle: as individuals, when interacting with artificial intelligence, it is imperative to be aware that we are engaging with a machine-driven intelligence."

National cooperation

"We lack the organic and multidisciplinary approach, that is, that within the administrations themselves, LEAs, for example, and judicial and prosecutorial authorities, form working teams, both for specific cases and for evaluation of these policies, to see how they work effectively over time."

European cooperation

"The challenge lies in the differences in legal culture among the 27 EU countries. Currently, we face difficulties, such as variations in investigative measures for communication interventions, like cross chat, where in France, prosecutors can authorize the police to use a Trojan, but not in Germany or Spain. Therefore, meaningful discussions are hindered due to the lack of total homogeneity."

Training to combat online trafficking

"We [victims' support organizations] are usually the entities that offer each other training, because the public authorities do not offer any training."

"We need to know more about the digital world [...] After Covid-19, places of exploitation have moved to digital. We urgently need this training."

Interrelation of online and offline trafficking

"Everything digital leaves traces, which allows us to know more things, we need to have the equipment to track and the regulatory tools to combat it. My impression is that the fight against human trafficking is happening in the natural world, but not in the digital world."

"The issue is having the technological capacity to access that information and then the regulatory instruments to be able to request it."

Conclusion

"Transform your problem into someone else's problem. Convince the EU that trafficking is a national security issue. While they may not launch missiles, the impact is similar. Psychological coercion is prevalent, making it a national security conflict that requires urgent attention."

3.4 Needs and Challenges:

Victim services

Victim services are two steps behind lacking training and tools on detection of human trafficking in the digital environment. Victim services need to be trained with the necessary skills in detecting and reporting digital trafficking. They lack protocols and tools.

One of the problems faced by victim services with sexually exploited women is that being foreigners, they have language and social barriers, they do not know the norm... it all starts with a sexual relationship, but then the exploitation takes place and they themselves do not know whether it is a sentimental relationship or exploitation.

Similarly, sexually exploited women are often on the move, and it is difficult to keep track them. They are also afraid of the police and expulsion, so they do not report these crimes.

Police & Authorities

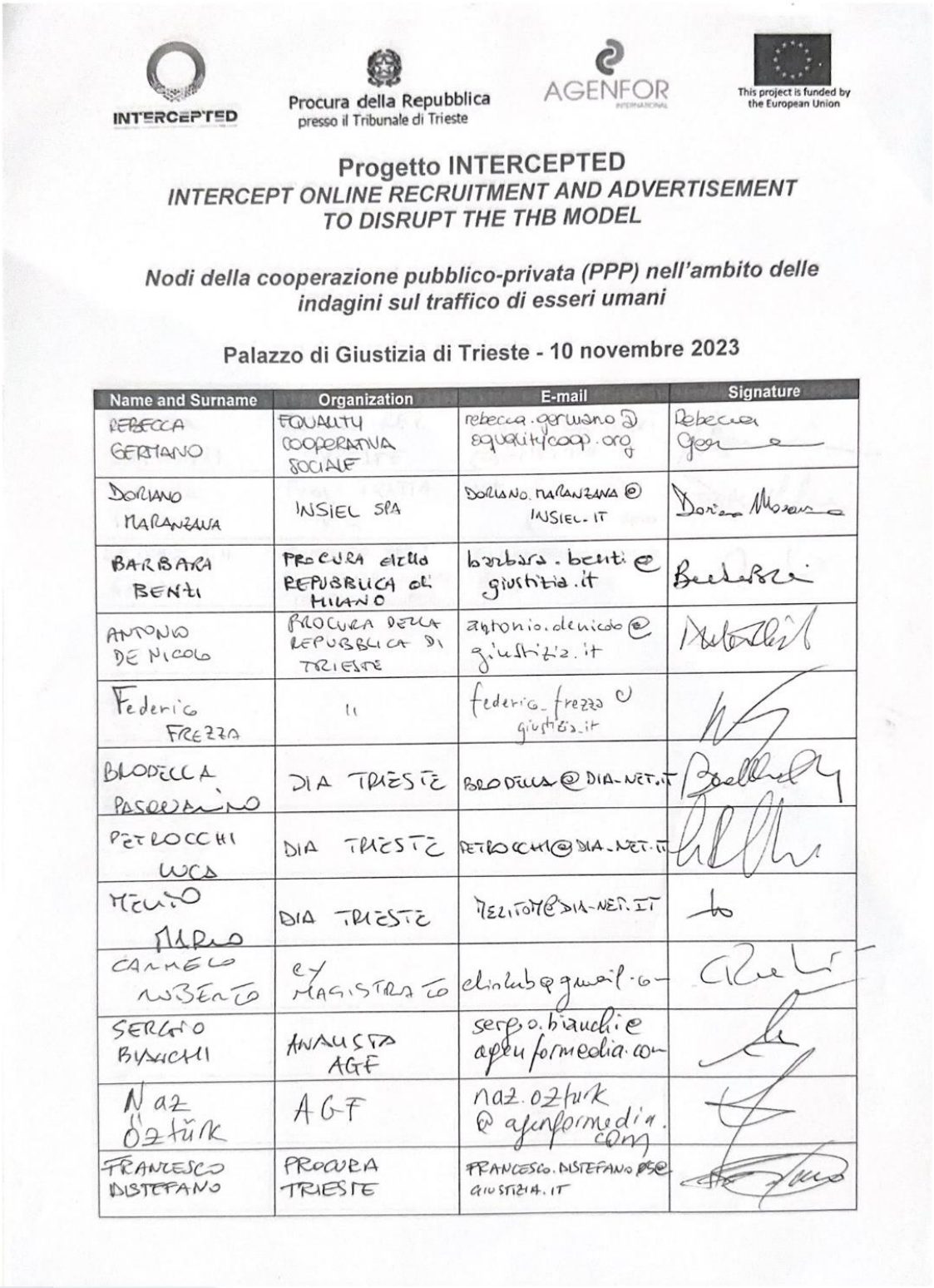
We also start from a problem of conceptualization in the police and authorities because it is difficult for them to understand trafficking as gender-based violence.

In addition, there is a lack of digital training for police officers on how the internet and cryptocurrencies work. In Granada, there is a scarce experience both in the police and in the Prosecutor's, Office investigating internet crimes on cases related to online human trafficking activities.

Regarding the administration of justice: online audio-visual material is often not accepted by the judge as evidence, as the judiciary is afraid to guarantee the authenticity and integrity of the digital document. There are digital notary services and other services that certify with a time stamp the time at which that document existed. When certified, that proof can be claimed. These are private resources (e-confianza).

The police can also call on them. However, online trafficking is handled by the Alien Section, but they are not computer literate. It is handled by the Computer Crimes Section, but the problem is that there is no collaboration between the different sections. In that sense, one could use as an example the policy adopted in Spain on hate crimes, where it has become a line of criminal policy, thanks to which LEAs have been properly trained, ad hoc police units have been created and protocols for action and cooperation have been established. There is an urgent need for training in cybercrime and teamwork between the different police sections, as well as to interrelate online trafficking with offline trafficking and with other crimes, especially financial crime.

4.Annex 1 – signature paper



INTERCEPTED

Procura della Repubblica
presso il Tribunale di Trieste

AGENFOR INTERNATIONAL

This project is funded by the European Union

Progetto INTERCEPTED
INTERCEPT ONLINE RECRUITMENT AND ADVERTISEMENT TO DISRUPT THE THB MODEL

Nodi della cooperazione pubblico-privata (PPP) nell'ambito delle indagini sul traffico di esseri umani

Palazzo di Giustizia di Trieste - 10 novembre 2023

Name and Surname	Organization	E-mail	Signature
REBECCA GERMANO	EQUALITY COOPERATIVA SOCIALE	rebecca.germano@equalitycoop.org	
DORIANO MARANZANA	INSIEL SPA	DORIANO.MARANZANA@INSIEL.IT	
BARBARA BENTI	PROCURA della REPUBBLICA di MILANO	barbara.benti@giustizia.it	
ANTONIO DE NICOLO	PROCURA DELLA REPUBBLICA DI TRIESTE	antonio.denicolo@giustizia.it	
Federico FREZZA	11	federico_frezza@giustizia.it	
BRODELLA PASQUALINO	DIA TRIESTE	BRODELLA@DIA-NET.IT	
PETROCCHI LUCA	DIA TRIESTE	PETROCCHI@DIA-NET.IT	
MELITO MARIO	DIA TRIESTE	MELITOM@DIA-NET.IT	
CARMELO ALBERTO	EX MAGISTRATO	elialab@gmail.com	
SERGIO BIANCHI	ANALISTA AGF	sergio.bianchi@agenformedia.com	
Naz Öztürk	AGF	naz.ozturk@agenformedia.com	
FRANCESCO DISTEFANO	PROCURA TRIESTE	FRANCESCO.DISTEFANO@GIUSTIZIA.IT	

INTERCEPTED | Procura della Repubblica presso il Tribunale di Trieste | AGENFOR INTERNATIONAL | This project is funded by the European Union

Progetto INTERCEPTED

INTERCEPT ONLINE RECRUITMENT AND ADVERTISEMENT TO DISRUPT THE THB MODEL

Nodi della cooperazione pubblico-privata (PPP) nell'ambito delle indagini sul traffico di esseri umani

Palazzo di Giustizia di Trieste - 10 novembre 2023

Name and Surname	Organization	E-mail	Signature
RENATA DAMIANI	PROCURA REP. TRIESTE	RENATA.DAMIANI @GIUSTIZIA.IT	
Daniela Manno	Prog. TRATTA F.V.G	art. 18fvg @ gmail.com	
LETONDE A.H. GBEDO	COMITATO PER I DIRITTI CIVILI DELLE PROSTITUTE APS	Stella polare.trieste @gmail.com	

(Focus Group Conducted online, the screenshot of the Teams Report)

Meeting duration 2h 47m 31s		
Average attendance time 1h 54m 8s		
2. Participants		
Name First Join Last Leave In-Meeting Duration Email Participant ID (UPN) Role		
Vagia Poutouroudi 11/21/23	9:32:26 AM 11/21/23	12:19:48 PM 2h 47m 22s v.poutouroudi@kemea-research.gr v.poutouroudi@kemea-research.gr Organizer
Katerina Georgakopoulou 11/21/23	9:32:46 AM 11/21/23	12:19:34 PM 2h 46m 48s k.georgakopoulou@kemea-research.gr k.georgakopoulou@kemea-research.gr Presenter
Andrianna Retzepi 11/21/23	9:35:10 AM 11/21/23	12:19:31 PM 2h 44m 20s a.retzepi@kemea-research.gr a.retzepi@kemea-research.gr Presenter
ΚΩΤΣΗ ΠΕΡΙΣΤΕΡΑ 11/21/23	9:54:05 AM 11/21/23	12:19:22 PM 2h 25m 17s Presenter
Κόκκινου Βαρβάρα 11/21/23	9:56:30 AM 11/21/23	12:10:32 PM 2h 14m 2s Presenter
Stavroula Spiropo - The Smile of the Child (Guest) 11/21/23	9:56:39 AM 11/21/23	9:58:04 AM 1m 25s Presenter
Lampros Tsogkas 11/21/23	9:58:08 AM 11/21/23	10:25:10 AM 27m 1s Presenter
Χαμογελο 11/21/23	9:58:29 AM 11/21/23	12:19:32 PM 2h 21m 3s Presenter
ΓΙΩΡΓΟΣ ΚΟΛΥΒΑΣ (Επισκέπτης) 11/21/23	10:00:22 AM 11/21/23	12:19:21 PM 2h 18m 58s Presenter
Άννα Ευθυμίου 11/21/23	10:02:11 AM 11/21/23	12:19:21 PM 2h 17m 9s Presenter
Γιαννοπούλου Ασημίνα 11/21/23	10:02:29 AM 11/21/23	12:19:19 PM 2h 16m 49s Presenter
Lampros Tsogkas 11/21/23	10:24:21 AM 11/21/23	12:19:33 PM 1h 55m 11s Presenter
Κόκκινου Βαρβάρα 11/21/23	12:10:59 PM 11/21/23	12:19:22 PM 8m 22s Presenter
3. In-Meeting Activities		
Name Join Time Leave Time Duration Email Role		
Vagia Poutouroudi 11/21/23	9:32:26 AM 11/21/23	12:19:48 PM 2h 47m 22s v.poutouroudi@kemea-research.gr Organizer
Katerina Georgakopoulou 11/21/23	9:32:46 AM 11/21/23	12:19:34 PM 2h 46m 48s k.georgakopoulou@kemea-research.gr Presenter
Andrianna Retzepi 11/21/23	9:35:10 AM 11/21/23	12:19:31 PM 2h 44m 20s a.retzepi@kemea-research.gr Presenter
ΚΩΤΣΗ ΠΕΡΙΣΤΕΡΑ 11/21/23	9:54:05 AM 11/21/23	12:19:22 PM 2h 25m 17s Presenter
Κόκκινου Βαρβάρα 11/21/23	9:56:30 AM 11/21/23	12:10:32 PM 2h 14m 2s Presenter
Stavroula Spiropo - The Smile of the Child (Guest) 11/21/23	9:56:39 AM 11/21/23	9:58:04 AM 1m 25s Presenter
Lampros Tsogkas 11/21/23	9:58:08 AM 11/21/23	10:25:10 AM 27m 1s Presenter
Χαμογελο 11/21/23	9:58:29 AM 11/21/23	12:19:32 PM 2h 21m 3s Presenter
ΓΙΩΡΓΟΣ ΚΟΛΥΒΑΣ (Επισκέπτης) 11/21/23	10:00:22 AM 11/21/23	12:19:21 PM 2h 18m 58s Presenter
Άννα Ευθυμίου 11/21/23	10:02:11 AM 11/21/23	12:19:21 PM 2h 17m 9s Presenter
Γιαννοπούλου Ασημίνα 11/21/23	10:02:29 AM 11/21/23	12:19:19 PM 2h 16m 49s Presenter
Lampros Tsogkas 11/21/23	10:24:21 AM 11/21/23	12:19:33 PM 1h 55m 11s Presenter
Κόκκινου Βαρβάρα 11/21/23	12:10:59 PM 11/21/23	12:19:22 PM 8m 22s Presenter

INTERCEPTED

FUNDACION EUROARABE

This project is funded by the European Union

GRUPO DE DEBATE - INTERCEPTED
Granada, 30 de Noviembre de 2023

Nombre y apellidos Name and Surname	Organización Organization	Email	Firma Signature
Habiba Hadjeb	Servicio de Protección de Menores	habiba.hadjeb@juntadeandalucia	
Ainhoa Rodríguez	Observatorio de la Infancia de Andalucía	ainhoa.rodriguez@juntadeandalucia.es	
Alexandra Andrea Toma Simian	Mujeres en Zona de Conflicto - Loja	alexandra.toma@m2c.es	
Karen hofl.	Fundea	Khofl@fundea.org	
ANA ISABEL CRUZ ORTIZ	APES "INTEGRA-2" CENTRO DE PROTECCIÓN DE MENORES	anaisabelcruzortiz@gmail.com	
Pablo M. Melgarejo Cordoba	Universidad de Granada	melgarejo@ugr.es	
FRANCISCO J. HERNÁNDEZ GUERRERO	MINISTERIO FISCAL ESPAÑA. FISCALÍA GRANADA	francisco.j.hernandez@fiscal.es	

AGENFOR · KEMEA · Procura della Repubblica presso il Tribunale di Trieste · HELLENIC POLICE · FUNDACION EUROARABE · HfÖ

5. Annex 2 – Consent form Template

(The consent forms haven't been attached to keep the report concise. They will be stored by Agenfor International and shared with the Commission if requested.)

INTERCEPTED FOCUS GROUP
Place, DD MONTH 2023

Organizer: partner

Consent Form

The Focus Group takes place within the INTERCEPTED, funded by the SF-2022-TF1-AG-THB program of the European Union under the Grant Agreement n. 101101938.
NAME OF THE ORGANIZER
Contact: email
Legitimation: the consent of the interested party
Subject: Implementation of the INTERCEPTED Focus Group
Recipient: partner.

Rights: Access, rectification, cancellation, limitation, potability and opposition.
Data Protection Officer:
The data used (name, surname, e-mail address) will not be published except for the purposes of the project.
Registration, publication and photos: activities could be registered to better enable implementation of the final report. The registration will not be used in any way for disclosure purposes and will not be published on any platform.
Further information:
To request more information on the processing of personal data and on the protection measures of your personal data, you can contact us at: email

I hereby confirm that	**YES**	**NO**
I have read and accept the processing of my personal data for the kick-off meeting		
I accept the terms of registration and participation in the kick-off meeting		

Name:
Signature:
Thank you for taking the time to complete this consent form. Please return it to the organizer.

6. Annex 3 – Invitation letter Template

Dear (insert name of participant),
We hope to find you well.

On behalf of the INTERCEPTED project Consortium, YOUR ORGANIZATION would like to inform that INTERCEPTED Focus Group, will be held on the dd Month 2023, from time, at place.

INTERCEPTED (*Intercept Online Recruitment and Advertisement to disturb the THB Model*) aims to disrupt the digital business models of trafficker by strengthening the digital capabilities of law enforcement and judicial authorities in the framework of public-private cooperation, through a better and unbiased understanding of the phenomenon, an enhanced capacity to stay on-top of online trends from a technological and a policing perspective, and new tools for the detection and responses of recruitment for and advertisement of trafficked services online, fully exploiting the potentiality of the OSINT-HUMINT-SIGINT cycles.

The Focus Group is dedicated to exchange of ideas and practices focusing specifically on advertisement and recruitment in order to effectively intervene to both supply and demand sides of THB (Trafficking in Human-Beings). The event will gather Law Enforcement Agencies (LEAs), Internet Service Providers (ISP), Judicial Practitioners and Victim Protection/Assistance Services to discuss the following topics related to the INTERCEPTED project:

- The needs of different stakeholders involved in THB by understanding the key trends in recruitment and advertisement of trafficked services online
- Existing trends in the recruitment of victims
- The differences in the way that different victim profiles and purchaser profiles are targeted differently online, considering both the type of exploitation (e.g., sexual, labour, and if labour, in what sector, e.g., agriculture, textile, construction) as well as the specific traits of the victims, such as age (/broad age category), gender, nationality, disability
- The ways in which different online platforms are used for the recruitment of victims of trafficking and the advertisement of their services

In this line, it is with great pleasure that YOUR ORGANIZATION invites you to participate in INTERCEPTED aforementioned event.

The INTERCEPTED Consortium is led by the Prosecution Office of Trieste (IT), and involves Center for Security Studies (EL), Hellenic Police (EL), AGENFOR International Foundation (IT), The Euro-Arab Foundation for Higher Studies (ES), and University for Public Administration in Bremen (DE).

If you are interested in participating in the INTERCEPTED Focus Group, please let us know by date.

Looking forward to hearing from you.

Kind Regards,
(Insert signature and name or organization)

Co-funded by
the European Union