TINERI CERCETĂTORI ŞTIINŢIFICI

CZU: 343.54:004.056
https://doi.org/10.52277/1857-2405.2024.2(69).09

EVERYTHING STARTS WITH A SIMPLE „HI” (NIJ TRAINEES AT THEMIS COMPETITION)

Authors:
Andrei DUBCEAC,
Cristian GURIN,
Sergiu NAZARENCO

Tutor:
Olga IONAŞ

SUMMARY

The development of information and communication technologies has changed the modus operandi of criminals. The Global Web became a means of committing crimes and a source of profits for offenders. This paper is based on the analysis of crimes related to the online sexual abuse of children, their investigation, and the issues related to investigating them. More recently, these crimes acquired a cross-border nature so the investigation process requires cooperation among institutions from multiple countries, which leads to various problems.

Key-words: *online child sexual abuse, CSAM, cross-border crime, data preservation.*

TOTUL ÎNCEPE CU UN SIMPLU „SALUT” (AUDIENŢII INJ LA CONCURSUL THEMIS)

SUMAR

Dezvoltarea tehnologiilor informaţiei şi comunicaţiilor a schimbat modul de operare a criminalilor. Web-ul global a devenit un mijloc de comitere a infracţiunilor şi o sursă de profit pentru infractori. Această lucrare se bazează pe analiza infracţiunilor legate de abuzul sexual online asupra copiilor şi problemele ce apar la investigarea acestora. Mai recent, infracţiunile respective au căpătat un caracter transfrontalier, astfel încât procesul de investigare necesită cooperare între instituţii din mai multe ţări, ceea ce provoacă diverse probleme.

Cuvinte-cheie: *abuz sexual online asupra copiilor, CSAM, criminalitate transfrontalieră, conservarea datelor.*

Introduction

Since the 1990s, information and communication technologies (ICT) have achieved astonishing growth resulting in accessible and numerous ways to communicate with other people and share information so it was a matter of time before ICT would be used in criminal activities at a large scale [2]. Disconnected personal communication, universality, low-cost standard and infinite virtual capacity are characteristics of the Internet that conditioned the use of ICT in criminal activities involving personal and lasting contact between victim and offender [7, p. 23].

The ubiquity of the Internet has brought a completely new chapter in criminal proceedings. The digital environment brought both benefits and obstacles to criminal investigations. The prosecution became able to bring in court digital evidence, got improved monitoring capabilities and gained new opportunities for undercover work. However, the main obstacles are the rapidly changing nature of technology and therefore of *modus operandi* of criminals, lack of monetary and human resources as well as lack of technological tools [12].

Online child sexual abuse is a broad term that encompasses various forms of sexual exploitation and abuse of children facilitated or carried out via digital technologies. This includes, but is not limited to, the production, distribution, and possession of child sexual abuse materials, online grooming, live

streaming of sexual abuse, and engaging children in sexually explicit conversations or activities online.

Key types of online child sexual abuse considered while writing this paper are:

Child Sexual Abuse Material or CSAM is a term that started to be used recently, it aims to replace the wide term „child pornography", last is considered inappropriate for depictions of sexually abused children because it makes a false impression of similarity between materials with adults involved in consensual sexual activities (pornography) and criminal conduct of abusing a child. In this paper is used the definition of CSAM from the proposal to amend the existing European Directive 2011/93/UE on combating the sexual abuse and sexual exploitation of children and child sexual abuse material which sets out that child sexual abuse material is "*any material that visually depicts a child engaged in real or simulated sexually explicit conduct; depiction of the sexual organs of a child for primarily sexual purposes; any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; realistic images, reproductions or representations of a child engaged in sexually explicit conduct or of the sexual organs of a child, for primarily sexual purposes and any material, regardless of its form, intended to provide advice, guidance or instructions on how to commit child sexual abuse or sexual exploitation or child solicitation*" [14].

Online grooming is the process where an adult builds an emotional connection with a child online to gain his trust in order to commit sexual abuse-related offenses. End-to-end encryption recently introduced by many popular messaging apps like Facebook Messenger, WhatsApp, Instagram etc. increases the privacy of communication between perpetrator and victim.

Live-streaming of abuse performed via video-calls is real-time broadcasting of the sexual abuse of a child, often orchestrated on demand for paying viewers. This kind of sexual abuse is particularly complicated to investigate due to little evidence left after and the cross-border character of streaming which usually involves a consumer from affluent countries like Europe, USA, Australia etc. and producers located in less developed countries. The only available evidence is previous discussions between the consumer and producer of CSAM (if they are not deleted) and financial transactions.

Before the expansion of ICT, the circulation of child sexual abuse material (CSAM) was a local matter, communication between producers and consumers or between consumers was time-consuming, dangerous and took place *via* conventional and easy-to-detect and intercept landmail. Nowadays connection to the Internet assures the access to global market of CSAM consumers.

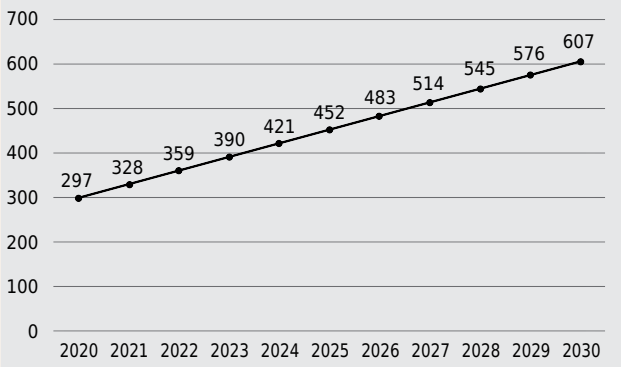

Fig. 1. Child pornography, number of offences per 100,000 population [16].

In 2013, children's rights activists from Terre des Hommes, a Dutch charity organization, created, using computer-generating tools, the image of a 10-year-old Philippine girl named "Sweetie" who, being controlled by an operator, was entering different chat rooms with strangers. Once the webcam conversation started, it went very quickly to explicit requests for various sexual performances. After this, the predator would make a money transfer and provide his ID from other platforms where broadcasting could be continued. Once the information was collected, the chat with Sweetie would be shut down and the information was provided to the law enforcement authorities. During only 10 weeks of operation, Sweetie avatar was contacted by more than 20 000 users from 71 countries, 1000 of whom were identified. Names, IP addresses and social media accounts were passed to Interpol [10]. Disregarding the fact that evidence provided by Terre des Hommes led to conviction in some countries, under the standards of ECHR this kind of activity, if led by an official undercover agent, could be an entrapment and therefore prohibited by art. 6 of the European Convention on Human Rights.

In the Republic of Moldova reliable macro-level data on the number of children using the internet and within what age bands, are not available. However, thanks to targeted individual studies a great deal is known about how Moldovan children use the technology, what benefits they derive from it as well as what problems they encounter. Unsurprisingly, the experience of Moldovan children mirrors more or less exactly the experiences of children everywhere else in Europe, and indeed around the world [8].

12% of children aged 9-17 years in Moldova received sexually explicit proposals on chats. 1 in 100 children sent sexually explicit content representing themselves to a person with whom they talked online. Globally, the COVID-19 crisis has resulted in a surge in the online distribution of child sexual abuse material, which was already at high levels before the pandemic [9]. According to EUROPOL, there have been significant increases

in activity related to child sexual abuse and exploitation, on both the surface web and dark web during the COVID-19 lockdown period. The increased number of offenders exchanging CSAM online may have an impact on and stimulate demand for this type of material online. At the same time, consistent levels of activity by offenders on the dark web during lockdown reflect the ongoing organized business model that has evolved and the level of threat that it poses to children. Moreover, lack of social awareness, outdated law provisions, underfunded law enforcement agencies and sporadic and isolated contacts between de facto authorities of Transnistria and moldovan authorities have led the Republic of Moldova to become a host for numerous web resources with CSAM worldwide available.

At the beginning of 2023, the first service of reporting the CSAM in the Republic of Moldova became operational and, in 6 months, in the period from 25 April to 25 October 2023, the service received 1997 reports which led to the removal of 3694 CSAM. 96,5% of reports contained CSAM, 2/3 of the victims were less than 13 years old and in 6 cases victims were less than 2 years old [1]. According to the Internet Watch Foundation Annual Report, in 2022 Republic of Moldova was on 11th place in the world by the number of hosted unique websites that disseminated CSAM [11].

The correlation between the preservation of evidence and respect for the rights of individuals

Every crime, regardless of its nature and specifics, must be proven, arising from the very purpose of the criminal process – to find out the truth. For the truth to be found out, the bodies empowered by law, namely the criminal investigation bodies, are to prove this fact through evidence, evidence that must be legally administered, be relevant, conclusive and useful to the case for ascertaining all the circumstances in which the act took place or did not take place.

Considering the fact that online child sexual abuse is a phenomenon that has been increasing in recent years, the specifics of these crimes require a much wider, more complex investigation and in the narrowest possible terms for the collection and preservation of evidence.

At the same time, throughout the process of preservation of evidence, the rights of individuals must also be taken into account. Here we are referring to victims who, given the specifics of online child sexual abuse, are minors and require a much greater treatment and guarantee of respect for their rights in relation to victims who have reached the age of 18. This fact emerges from the Lanzarote Convention [4], which in article 30 states that "Each Party shall take the necessary legislative or other measures to ensure that investigations and criminal proceedings are carried out in the best interests and respecting the rights of the child."

The first step – the voice of the victim

At the initial stage, when the criminal investigation body is notified in the manner provided by the law about the commission of sexual abuse in the online environment against minors, it has the obligation to ensure the hearing of the victim before the investigating judge, the hearing being audio-video recorded, in the presence of the victim's lawyer, the psychologist and other participants in the case, the de facto hearing being conducted through the psychologist, the questions given by the parties being prepared ahead of time. In the national law of the Republic of Moldova, this procedural action is provided by art. 110^{1} Criminal Procedural Code of the Republic of Moldova. In such circumstances, cumulatively several conditions imposed by the national law but also by the conventions and treaties to which it is a party will be met.

First of all, the hearing of the injured party under special conditions before the investigating judge represents evidence that will be administered legally and in the shortest possible time, the victim being able to tell in detail all the circumstances necessary for the case. Moreover, hearing the victim as soon as possible reduces the possibility of influencing the statements given by her later, the influence being possible both on the part of those in whose care they are or the legal representatives of the victim being influenced by the suspect.

In case 1ra-442/2022 [15] regarding B. based on art. 208/2 Criminal Code, the minor victim (16 years old), gave statements several times during the criminal prosecution phase, until the changes of 09.01.2023, the statements not being recorded on video.

Thus, in the first statements, the minor victim indicated that B. was sending her voice recordings with a sexual tone, porn videos and photo images of a sexual nature via ICT, with the aim of maintaining sexual relations, he tried to rape her".

Later, the victim was interviewed repeatedly, declaring, "that the sexual acts took place with his consent, for sums of money offered by B.".

As we can see in the case mentioned above, the victim was not heard under special conditions, her hearing was not recorded and she was going to make repeated statements during the criminal investigation phase, all statements being called into question.

More than that, as we saw in the case mentioned above, the minor victim was interviewed several times during the criminal investigation phase, a fact that was not going to happen in any case or according to Art. 31 lit. f) of the Lanzarote

Convention – *„Each Party shall take the necessary legislative or other measures to protect the rights and interests of victims, including their special needs as witnesses, at all stages of investigations and criminal proceedings, in particular by providing for their safety, as well as that of their families and witnesses on their behalf, from intimidation, retaliation and repeat victimization”*. States must adopt and harmonize domestic legislation in such a way that victims of sexual crimes are not subject to re-victimization.

With the hearing of the victim under special conditions, the rights of the suspected person will be guaranteed and respected, or he will have the opportunity to view the video recording of the hearing of the victim, having the possibility to ask those questions that were not clarified during the hearing. The repeated hearing of the victim will be conditional on the fact that all aspects and circumstances of the case have not been elucidated, this being an exception based on the principle of non-revictimization.

Cross-border character – where issues arise

Data preservation does not compel either collection or retention of data; it is essentially a “do-not-delete” order pertaining to existing data. A data preservation scheme provides that upon a lawfully authorized request, based on the facts of a specific case, particular data that has already been collected can be preserved to prevent its deletion. At a later point, a lawful request by a competent authority can compel disclosure of the data.

The problem that often arises in practice concerns the fact that the same illegal action in two different states qualifies differently under national law. Thus, if in one state a CSAM action can be qualified as a serious crime, in another state, to be requested by the first state, the given action represents a less serious, light or generally is not provided as a crime, a major problem arises with regard to the preservation and collection of evidence. As a result, the requesting state is unable to conduct an effective investigation, which in itself leads to a multitude of violations of the victim’s rights.

In the same context, there are problems even between jurisdictions with the same degree of harmonization of national legislation in relation to international regulations, and here we are mostly talking about European states. The problems essentially increase between states with different domestic legislation from one another, thus, due to the fact that there is no harmonization regarding the regulations regarding the qualification of actions related to CSAM, difficulties arise when requesting international legal cooperation in the matter criminal, being, however, necessary a double criminalization of the actions in both states involved.

A solution in this regard is the harmonization of legislation regarding the legal classification of the facts, that is, the same action has the same qualification regardless of the state.

By the Convention on Cybercrime, upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve promptly the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition for providing such preservation.

Preservation must be possible for electronic evidence in relation to any criminal offences. It is a provisional measure, and it must be possible in the first step to order the preservation of volatile data without delay.

The preservation will then allow for the time needed for the second step, that is, to actually obtain the data through formal procedures, such as search and seizure or production orders which in most countries require a court order.

By the convention, Parties should take measures in order to save cyber data for not less than 60 days, which implies that regardless of whether or not the state was requested to preserve the computer data, the providers are to keep this data for 60 days. Even if it is established that states are to keep the data for a period of no less than 60 days, some states, based on internal laws, have modified this term.

So, each state has its own domestic regulations regarding data retention periods, which in itself is a major problem. Once a request for the preservation of evidence has been made, the next step will be to make a request for the collection of evidence, but given the fact that the national regulations for authorizing a measure for the collection of evidence in another state, which in itself requires time. At the same time, the fact that each individual state has its data retention period, especially those that do not have a deadline, the probability of losing evidence is real, considering the fact that these are volatile evidence, evidence that has a deadline keeping very narrow.

More than that, the fact that rogatory commissions are very difficult to execute, the risk of losing evidence, especially in the situation where the period of preservation of cyber evidence is different or does not exist, the probability of the subsequent collection of the evidence decreases significantly. We cannot speak of an effective investigation if we cannot preserve evidence that has not been preserved, nor can we collect evidence that does not exist.

Transnistria – de jure and de facto

The topic of preserving evidence from Transnistria is a complex challenge from a political, legal and practical point of view. Located between Moldova’s eastern border and the Dniester River, the

Transnistria region is characterized by a disputed status and separatist control exercised by a self-proclaimed entity, the Moldavian Dniester Republic (Transnistria). This complicated situation generates significant difficulties regarding the preservation and management of evidence in the context of judicial processes and criminal investigations. One of the main problems is represented by the legal and jurisdictional authority over Transnistria. The lack of international consensus on its status and limited global recognition creates a legal vacuum, which can affect the application of international and regional standards regarding the preservation of evidence. This can lead to the risk of loss or degradation of evidence crucial to investigations and legal proceedings.

A very important point is the fact that the constitutional authorities of the Republic of Moldova are prohibited from cooperating with the authorities on the left side of the Dniester and even with the providers in the region. The problem is that even if the national authorities of the Republic of Moldova directly address to the providers from Transnistria, this is not valid either, although the providers, as defined by the Budapesta Convention, are internet service providers, but given that Transnistria is an autoproclaimed state that does not a part of the Convention, it is impossible to request information from them. It is not even clear whether, according to their domestic laws, the providers are obliged to keep the information, if so, then what is the retention period?

From another point of view, the criminals living in Transnistria know about the fact that Transnistria is an inaccessible place from the point of view of international investigations, they know about the fact that the possibility of their being caught is small, if not impossible and they know about the fact that both their authorities and providers cannot release information about their identity, about the history of actions carried out in the online environment. Thus, part of the sites with CSAM materials are hosted on the territory of Transnistria. Not only is it impossible to carry out any actions on the territory to the left of the Dniester, but the very people involved in CSAM know about this fact and intensively abuse it.

The problem of the fact that the CSAM materials are hosted on the territory of Transnistria is a problem that refers to the global society, or the CSAM materials through Transnistria are distributed all over the world, and considering the fact that the prevention of such crimes is one of the basic points in the fight against online child sexual abuse, we cannot talk about effective prevention at a time when no state can legally act, preserve, administer or collect evidence from the territory of Transnistria. Concerning the given fact, the tendency to attract other people as authors or consumers increases or demand creates supply. At the same time, the fact that a fairly large percentage of crimes related to online child sexual abuse are committed for financial reasons, Transnistria became an "Eldorado" for those who deal with CSAM.

What can we do in the above-mentioned situation? In our view, a solution to the problem could be cooperation with international organizations, such as the OSCE, which proposed, as one of its missions, the efficiency of cooperation between the Republic of Moldova and Transnistria, the guarantee of respect for human rights, as well as the consolidation of policies, measures and access to damage recovery in order to support victims and prevent exploitation on both banks of the Dniester River [5]. We should also mention that human rights and the well-being of society should prevail over political disagreements.

Methodology of investigation

In terms of victims and the challenges in identifying them, it's crucial to understand that children who are exploited or abused online can come from diverse backgrounds. The nature of online abuse can make it particularly challenging to identify victims since the abuse can occur in the privacy of the child's home, often without the direct knowledge of caregivers or others who might typically observe signs of abuse.

Online child sexual abuse and exploitation present a significant challenge, as victims are often hesitant to report the abuse committed against them. Children may be afraid of being blamed for sharing or engaging in sexual activities online, feel ashamed, or fear being stalked due to digital evidence of their abuse circulating online. Despite legislation and international standards, such as the Lanzarote Convention, which require law enforcement to investigate presumed cases of sexual abuse, regardless of whether the victim has made a report or accusation, this standard is not always upheld in practice. Unfortunately, law enforcement and the justice system often place the burden of proof on the victims themselves. Investigations typically start with a tip or report made to law enforcement agencies or online platforms. Following this, digital forensics is a critical component, where experts analyze digital devices and online accounts to uncover evidence of abuse or exploitation. Cooperation with internet service providers and social media platforms is often necessary to trace the source of abusive content or identify the abuser.

Law enforcement employs several modern techniques and analytical tools to combat online abuse. However, abusers have become adept at concealing their digital footprints and operating in virtual environments with an increased level of anonymity. This trend highlights the urgent need

to upgrade investigative tools by incorporating Artificial Intelligence and automating investigation processes. By doing so, investigative officers can search, choose, and document cases more efficiently by analyzing a large volume of information on online activities. This will enable them to identify possible similarities in the way the abuse is committed and track the actions taken to identify online sex abusers.

Investigating online sexual abuse and exploitation crimes requires thoroughly examining both the physical and digital crime scenes. Evidence is collected from the physical environment on the physical scene, and evidence is extracted from the hardware and software components on the digital scene. It is essential to investigate both scenes to ensure a comprehensive analysis of the crime or incident.

The current legislation does not offer a definitive solution to halt the spread of child sexual abuse materials across all online platforms, nor does it outline concrete investigative measures that should be taken in cases of live streaming, sexual extortion, or other forms of abuse. As a result, it is possible for the abuse to continue even after the child has lodged a complaint with the police, and no real steps are taken to shield the child from further contact with the perpetrator online.

Republic of Moldova – institutions and case studies

In the Republic of Moldova, the investigation of online child sexual abuse is made by the „National Investigation Inspectorate" which is a part of the General Police Office – a specialized public institution of the state, under the Ministry of Internal Affairs.

The National Investigation Inspectorate works with the Prosecutor's Office, represented by a specialized section on cybercrime within the Prosecutor's Office for Combating Organized Crime and Special Cases.

They have the mission to detect, investigate, and uncover particularly serious and exceptionally serious crimes, as well as those with significant social impact, to follow and hold accountable particularly dangerous offenders, to organize, conduct, and direct special investigative activities, and to monitor organized crime.

Investigating online child sexual abuse requires a nuanced understanding of digital environments and the use of specialized investigative techniques. Law enforcement agencies employ a variety of methods to detect, investigate, and prosecute cases of online child sexual abuse. These methods include cyber patrolling, digital forensics, undercover operations, and the use of online monitoring tools. Investigators often rely on sophisticated software to trace the digital footprints left by offenders on the internet, enabling them to uncover identities, gather evidence, and link suspects to criminal activities.

One of the primary challenges in investigating such cases is the collection and preservation of digital evidence. Digital evidence is volatile and can be easily altered or deleted. Investigators must act swiftly to secure this evidence while adhering to stringent legal and procedural protocols to ensure its admissibility in court. Additionally, the anonymity afforded by the internet complicates the process of identifying both perpetrators and victims. Offenders often use encryption, the dark web, and other methods to conceal their identities and activities, making it difficult for investigators to trace and apprehend them.

Case 1 „From digital shadows to dire reality"

In one of them, „Michael" was to obtain pornographic material from „Alice" and sexually exploit her, involving forced sexual acts and their recording. „Michael" used emotional manipulation, threats to disclose intimate material, and physical and mental violence to control the victim. The exploitation included transporting „Alice" abroad and forcing her to participate in sexual acts, recording these encounters. Law enforcement has encountered challenges in collecting and analyzing evidence, including digital communications and video footage. The investigation required a meticulous approach to corroborate „Alice's" testimony and gather compelling evidence against the accused.

The case involved multiple forms of abuse, including physical and psychological violence, threats with a weapon, sexual abuse and violence, taking advantage of the victim's vulnerability, and threatening to disclose confidential information. Law enforcement had to collect and analyze a variety of evidence, including digital communications through social networks and applications, video recordings, and the testimonies of victims and witnesses. This required technical knowledge and meticulous coordination. Due to the sensitive nature of the case, it was essential to ensure adequate protection and support for „Alice", adding an additional level of complexity to the investigation. „Michael" used manipulation and intimidation to control „Alice", making the gathering of direct and convincing testimonies even more difficult.

Case 2 „Echoes of the screen"

The next case refers to a serious situation of sexual exploitation of a minor, in which „Victor" was involved in human trafficking activities.„„Emily", who was a minor was recruited and sheltered for the purpose of commercial sexual exploitation, involving elements of deception, physical violence, and threats.

„Victor" emotionally manipulated the victim, taking advantage of the emotional attachment and the couple's relationship to control and sexually exploit her. „Emily" was forced to perform online sexual services through information technology such as web chats on various sites, where she was exposed in indecent poses and engaged in sexual acts in front of the camera. „Victor" used physical and psychological violence, including beatings and threats to release compromising material, to maintain control over the victim. Through this exploitation, „Victor" obtained significant amounts of money, while „Emily" was left in a state of vulnerability and lack of support. The trauma and psychological impact on the victim is obvious, with long-lasting effects on their mental health and well-being.

Case 3 „The virtual predator"

In the next case „John" – the abuser had the intention of determining a minor – „Laura" to sexual relations and other actions of an unwanted sexual nature, acting intentionally, using various messaging applications, and disguising his identity by using fake accounts on social networks. Under the invented pretext that he represents an agency of photo models and will hire her to work as a photo model, requested „Laura" to send him pictures of her in underwear. Continuing his criminal intention, during the same period of time, „John" wanted to determinate „Laura" to have sexual relations and other actions of an unwanted sexual nature with him, threatening her that he would divulge the intimate pictures and videos that he previously obtained to her family and other people and even would spread them in the online environment. That led „Laura" to continue taking intimate photos and participate in video sessions of intimate character.

The cases of online child sexual abuse are a transnational issue that requires a coordinated response from both national and international law enforcement agencies. At the national level, specialized units such as Internet Crimes Against Children task forces are essential. These units possess the expertise and technology needed to conduct investigations in the digital realm.

Internationally, organizations like INTERPOL and Europol play critical roles in facilitating cooperation and information sharing among countries. They offer platforms and databases for exchanging information about cases, suspects, and victims, enhancing the ability of national agencies to pursue cross-border investigations.

Conclusions

The detailed examination of the accused's electronic devices, such as mobile phones and computers, was required to extract images, videos and other relevant data, as well as the analysis of the accused's communications and online interactions is difficult due to the encryption of devices, requiring time and specialized expertise to access and examine their contents, essential for evidence collection.

Psychological assessment reports of the victims showed signs of psychological trauma, indicating the profound effects of abuse and exploitation on their mental health. This aspect was crucial in understanding the impact of the crime on the victims and required a sensitive and psychologically informed approach to the investigation. It is important to evaluate the risks for victims and ensure crisis intervention to protect children's interests. The investigation of these crimes is usually oriented toward protecting the suspect's rights and the presumption of innocence rather than securing the child victims who usually are in close relationships with their abusers, having emotional and psychological connections with them as a result of manipulation.

The first steps toward fixing the issues

The current legal framework confers the EU Member States the burden of designing and implementing prevention policies according to their cultural and societal environments and needs. As mentioned above, the number of online sexual offences is growing and trends are concerning so there is a demand for a centralized response to the new reality. The first step towards centralization will be the creation of the EU Centre – a community agency with a supportive role for national judiciary authorities in combatting child sexual abuse.

Given the specifics of CSAM-related crimes, a considerable problem is the fact that arresting the perpetrator and confiscation of materials held by him doesn't ensure that the same materials are excluded from the Global Web and re-victimization is therefore avoided. The only solution for prevention is evaluating and filtering the content before it is uploaded to the Internet or problems scaled by technology should be solved using technological solutions. There are different approaches regarding CSAM and child protection online from leading tech companies. Some of them went for on-device solutions to ensure privacy for every user [3], another opted for tools to detect CSAM like PhotoDNA and in-product reporting tools available in their soft [13]. While the efficiency of these tools is undoubted, they remain a private and optional initiative used only in their products.

A proactive and preventive approach to combating sexual abuse and exploitation of children should be considered. By focusing on individuals who recognize their potential risk of committing such offenses, we should aim to intervene before any harm can occur. We should also consider the

importance of early intervention in preventing potential offenders from acting on harmful impulses. By providing access to prevention programs, individuals can receive the support and intervention they need to prevent the commission of offenses. The inclusion of prevention programs underlines the recognition that potential offenders may need mental health support and intervention. Another proposal is the revision of the provisions member states must incorporate into their national laws. This clarity is crucial for ensuring that all member states understand and apply the changes consistently. By specifying the provisions that need transposition, the amendment aids in creating a more consistent legal framework across the EU. This consistency is vital for addressing cross-border challenges of child sexual abuse and exploitation, ensuring that offenders cannot exploit differences in legal standards between countries.

A significant element of CSAM-related offenses is the payments made to producers and distributors. While some of the perpetrators share possessed CSAM in exchange for new CSAM from other participants, the most serious and abhorrent materials are usually distributed in exchange for a one-time payment or based on monthly or annual subscriptions. Tracking the money would be a solution to tackle this particularly dangerous crime. At the moment, law enforcement authorities are able to access the information on a case basis through court orders when there is already evidence regarding the existence of the offence, so they don't take account of the offenders without criminal records. It was demonstrated that is possible to identify offenders only based on financial activity [6]. Creating the financial profiles of offenders by deeper cooperation between law enforcement authorities and financial institutions would provide new possibilities in identifying perpetrators and preventing them from further demanding of new CSAM. This approach applies to cryptocurrency also because many law agencies are able, with an additional effort, to track such transactions.

Another source of CSAM is self-produced materials. Preventing them from being uploaded to the Internet will decrease the total volume of CSAM available online. Preventing policies should aim children, their parents and professionals who interact everyday with children – teachers, social workers, psychologists and others. It is important to raise awareness about the consequences of sharing explicit photos or videos and the fact that child sexual abuse is much more prevalent on the Internet than we think. Everyone could become a victim.

Refferences

1. *Abuzul sexual* în *mediul online se* întâmplă *mai des decât ne imaginăm*. https://lastrada.md/rom/articole/abuzul-sexual-in-mediul-online-se-intampla-mai-des-decat-ne-imaginam-379 (visited 01.05.2024).
2. According to INTERPOL Annual Report for 2022, Online Child Sexual Exploitation and Abuse is considered a top crime threat along with money laundering, ransomware, phishing and online scamms, financial fraud, synthetic drug trafficking, organised crime and cannabis trafficking.
3. Apple's Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy. https://www.wired.com/story/apple-csam-scanning-heat-initiative-letter/ (visited 01.05.2024).
4. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse Lanzarote, 25.X.2007. https://rm.coe.int/1680084822 (visited 22.04.2024).
5. Crime victims' rights to rehabilitation and compensation – Guide. Chişinău, 2022. https://www.osce.org/ro/mission-to-moldova/525762 (visited 01.05.2024).
6. Cubitt T., Napier S., Brown R. *Predicting prolific live streaming of child sexual abuse*. Trends & issues in crime and criminal justice, 634, Australian Institute of Criminology, 2021.
7. Davidson J., Gottschalk P. *Characteristics of the Internet for criminal child sexual abuse by online groomers*, Criminal Justice Studies: A Critical Journal of Crime, Law and Society, 24:1, 2011, p. 23-36.
8. https://lastrada.md/pic/uploaded/COS%20Research%202021_summary.pdf (visited 22.04.2024).
9. https://lastrada.md/pic/uploaded/Studiu_Siguranta_online-comportamente_si_riscuri-FINAL.pdf (visited 25.04.2024).
10. https://www.vice.com/en/article/438m89/computer-generated-10-year-old-girl-ignites-ethical-debate-with-first-pedophile-conviction (visited 22.04.2024).
11. Internet Watch Foundation Anual Report 2022. https://annualreport2022.iwf.org.uk/trends-and-data/geographical-hosting-domains/ (visited 25.04.2024).
12. Mitchell K.J., Boyf D. Understanding the role of the technology in the commercial sexual exploitation of children: the perspective of law enforcement, Crimes against Children Research Center, University of New Hampshire, 2014.
13. Microsoft's practices on protecting children. https://www.microsoft.com/en-us/corporate-responsibility/digital-safety-content-report?activetab=pivot_1%3aprimaryr3 (visited 23.04.2024).
14. Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA.
15. The Decision of the Supreme Court of Justice nr. 1ra-442/22 of 04.05.2022. https://jurisprudenta.csj.md/search_col_penal.php?id=21069 (visited 22.04.2024).
16. United Nations Survey of Crime Trends and Operations of Criminal Justice Systems (2018 UN-CTS). https://www.unodc.org/unodc/en/data-and-analysis/United-Nations-Surveys-on-CrimeTrends-and-the-Operations-of-Criminal-Justice-Systems.html (visited 25.04.2024).