National concept for systemic solutions to combat child sexual exploitation and abuse

Junior Inspector (Ret.) Katarzyna Staciwa, M.A.[1]

[1] NASK - National Research Institute, Department of Response to Illegal Content on the Internet, Dyżurnet.pl, katarzyna.staciwa@nask.pl, ORCID: 0000-0003-0633-4696

Summary

Sexual exploitation and abuse of children in cyberspace, including the presence of content that is a visual record of criminal acts committed against them, is a global problem. The fight against this problem is effective when the actors involved make systemic use of the available technological solutions. This applies in particular to solutions that allow for a quick verification of whether potentially illegal content has been previously classified as Child Sexual Abuse Material (hereinafter: CSAM), as well as to communication between persons accessing such content in the course of their duties.

This study aims to provide an overview of solutions and tools used in this area, both internationally and nationally, and to propose a systemic approach that will contribute to the effectiveness of current solutions in the above area at national level.

Key words: child sexual abuse, child sexual exploitation, cyberspace, Child Sexual Abuse Material, CSAM, hash values

Introduction

The expansion of the Internet computer network in recent years, as well as the increasing number of mobile devices communicating with it, has undoubtedly had an impact on many areas of life in today's society, which is not without reason described as a global village. Technological progress, now an integral part of our lives, has caused that many phenomena occurring in the real world have moved into cyberspace. As J. Wasilewski aptly notes, the essence of the latter "is formed by the concept of bringing to life a kind of parallel environment, which is a new dimension for human activities" (2013). The trend indicated here also applies to the phenomenon of child sexual exploitation and abuse, where the actual behaviour is captured in photographs and videos, which are then distributed digitally between recipients who fall into a particular category of cyberspace users.

The offline and online dimensions have been linked in a particular way. This link has been described in research, for example, by Seto, Hanson and Babchishin (2010), indicating that about 55% of perpetrators operating in the virtual world admitted to sexual abuse of children in reality, and 12% of such perpetrators had a previous criminal record in connection with so-called contact crimes. In contrast, the American non-profit organisation, Child Rescue Coalition (hereafter: CRC), known for providing technological solutions to support law enforcement, indicates the percentage of so-called contact perpetrators in the group of perpetrators operating in the virtual world at 85% (2021).

To illustrate the scale of this phenomenon, it is worth recalling here the facts of the darknet platforms shut down as a result of international law enforcement operations in 2017.[1] These platforms brought together individuals with a sexual interest in children, enabling them to communicate directly, including the distribution of CSAM and the transmission of child sexual exploitation and/or abuse in real time, characterised by a high degree of anonymity. According to information provided by the European Cybercrime Centre (hereafter: EC3), operating within the structures of the European Union Agency for Law Enforcement Cooperation based in the Hague (hereafter: Europol), these platforms ranged from tens of thousands (Elysium platform, over 87,000 users) to even several hundred thousand of users (Playpen platform, over 150,000), (2017).

Information on current trends regarding the phenomenon of child sexual exploitation and abuse in cyberspace can be obtained from reports published by agencies and organisations specialised in this field,

[1] Dark web - is, in simple terms, a hidden part of the Internet resources that can be browsed using special software. The Darknet, on the other hand, is a restricted access network consisting of many distributed, anonymous nodes (such as Tor, I2P or Freenet) that allow access to the dark web.

such as Europol, (2020 and 2021) or the Council of Europe (2021). In these reports, one can observe a breakdown of trends into:

- trends concerning the content of CSAM category and
- trends concerning behaviour in cyberspace (e.g. grooming, solicitation or sexual blackmail).

The results of the analysis of these trends give rise to the conclusion that the phenomenon of child sexual exploitation and abuse will never be completely eliminated from cyberspace, but efforts can and should be made to reduce its scope and scale, although this task too is undoubtedly already a huge challenge. For the most part, these efforts are being made through the use of solutions to quickly verify whether potentially illegal content has already been classified as CSAM, as well as through communication between persons accessing such content in the course of their duties. It should also be noted that attempts are being made to implement solutions using artificial intelligence to identify dangerous online behaviour towards children, such as grooming (Microsoft, 2020). This study takes a closer look - based on the method of analysis and review of literature - at the functioning of solutions referring to the first of the above-mentioned trends, as well as proposes a systemic approach that could improve the effectiveness of current solutions in this area in Poland.

CSAM as a current challenge

The discussion of the first trend mentioned above should start with the thesis that the demand for the availability of child sexual exploitation and abuse content in cyberspace exists i.e. when the users in cyberspace are sexually interested in children persons, especially those who have conditions to commit sexual offences and record them on video. While it is beyond the scope of this paper to provide a full characteristics of such individuals, it is worth noting here that their possession of a new CSAM photograph or video, previously unpublished anywhere else, is a kind of trophy and currency for them (Europol, 2015). The use of the latter can, for example, make it possible to 'move up' in the hierarchy of covert forums on the Internet or gain access to private groups that disseminate, including by live streaming, strictly defined content, often depicting the most brutal and sadistic treatment of a sexually exploited and/or abused child.

It is impossible to estimate how much CSAM is currently available in cyberspace. In its recent publications, Europol once again points to a sustained year-on-year increase in the amount of CSAM content revealed in cyberspace, which naturally translates into its continued distribution and redistribution (Europol, 2020). As estimated by other experts in this field, a single image or video depicting the sexual exploitation and/or abuse of a child can be viewed or shared online up to 70,000 times (Web-IQ, 2020). A figure in excess of 2.5 million can provide another benchmark in efforts to determine the scale of the problem - this refers to IP addresses that have been linked to one of the most commonly shared CSAM category files in cyberspace (CRC, 2021).

An organisation with a special mandate to prevent and combat child sexual exploitation and abuse is the National Center for Missing & Exploited Children in the United States (hereafter: NCMEC). It has within its resources the CyberTipline, i.e. a hotline which is affiliated - like the other 50 hotlines operating in different parts of the world - to the INHOPE association (INHOPE, 2021). Under US federal law, local private sector entities are required to report to CyberTipline incidents of content in their resources that may depict child sexual abuse. This is a unique regulation, with no equivalent anywhere else in the world to date. The figures published by the organisation are alarming: in 2020 CyberTipline received more than 21.7 million such reports, a 28% increase compared to 2019 (2020). In 2021, there was another increase in the number of reports - to 29.3 million (up 35% from 2020), (NCMEC, 2022).

The description of a challenge posed by the presence of CSAM in cyberspace should be concluded by recalling the perspective of the victims of a crime in this category. Studies conducted with these individuals have repeatedly shown that the digital distribution of CSAM exacerbates their victimisation and has a long-term detrimental impact on them even when they reach adulthood (e.g. Canadian Centre for Child Protection, 2017). According to the Centre's survey, 70% of this population are constantly afraid of being recognised in real life. It is therefore the responsibility of the society in which children grow up not only to protect them from sexual exploitation and/or abuse in the real world, but also from experiencing secondary victimisation caused by availability in the virtual world of evidence of an offence committed against them.

Technology on duty

Verification of potentially illegal content by comparing *hash* values assigned to it is nothing new. The use of this method in preventing and combating child sexual exploitation and abuse has already been subject of numerous scientific (e.g. Quayle, 2020; Lee, Ermakova, Ververis, Fabian, 2020; Elshenraki, 2021) as well as expert (e.g. European Commission, 2020; Council of Europe, 2021) publications. This study draws on content from such publications, focusing on the practical side of using this method as a key element in a systemic approach that could be implemented at national level in Poland.

An in-depth analysis of the processes involved in assigning a *hash* value is not the purpose of this paper. At this point, however, it will be useful to clarify that such a value is nothing more than a sequence of digits and characters calculated using various

algorithms (e.g. MD5, SHA-1, PhotoDNA, pHash, TMK PDQF, SIFT), (e.g. Staciwa, 2021; Council of Europe, 2021), so more precise definitions would be the value of a one-way encryption function or the value of a cryptographic hash function (CHF). Since a *hash* value is unique for each file, it is equally often referred to as a 'digital fingerprint'.

The use of the method described here is extremely valuable for all actors involved in identifying child victims of sexual exploitatioin and abuse and combating the availability of CSAM in cyberspace. It is through this method that it is possible to quickly determine whether there is CSAM content in a large collection of digital material. This verification method is the basis for the operation of a special database held by the INTERPOL International Criminal Police Organisation with its headquarters in Lyon (the International Child Sexual Exploitation Database, hereinafter: ICSE DB). The ICSE DB is primarily a platform that enables investigators from more than 68 countries around the world to share criminal intelligence information about their cases. Transfer of content to the ICSE DB makes it possible to verify whether such content has already been identified in another country, as well as whether it bears similarities to other content already in the database, which as of today numbers more than 4.3 million images and videos (INTERPOL, 2022). Verification described here is invaluable for investigators, as it means being able to determine whether the material they are dealing with is new, which justifies the suspicion of real-time sexual exploitation and/or abuse of a child and involves prioritising such a case. Part of the ICSE DB is software that compares images and video so that investigators can establish links between victims, perpetrators and crime scenes in real time. The fact that cooperation of the international investigative community since the inception of ICSE DB has led to identification of 32 700 children worldwide should be an argument for the validity of solutions discussed here (INTERPOL, 2023).

An additional benefit of the classification described here is that a person dealing with potentially illegal content will not have to look again at content that has already been classified, which in practice amounts not only to avoiding duplication of work for those dealing with such content, but also to reducing the amount of time they are exposed to it. Exposure to such special content is highly stressful and, in the interests of the mental and physical well-being of such persons, contact with it should be kept to a minimum.

The creation of reliable lists of *hash* values attributed to CSAM category content and the exchange of information about these values are an invaluable contribution to the efforts of the international community involved in countering the availability of CSAM in cyberspace. The knowledge and experience of those dealing with this type of content as part of their duties, acquired, among other things, in training courses organised by INTERPOL, as well as the possibility to cooperate with other actors at a global level, are elements that enhance the effectiveness of these efforts.

It is worth mentioning at this point that solutions based on the technology described here have long been used by some law enforcement agencies, especially those with national CSAM databases, such as those in Sweden or the UK, as well as those that cooperate on a daily basis within the ICSE DB. The list of entities that use *hash* values in their daily work is further supplemented by some of the hotlines involved in removing illegal content from cyberspace: CyberTipline - United States, Cybertip!ca - Canada, Internet Watch Foundation (hereafter: IWF) - United Kingdom and, more recently, also Meldpunt Kinderporno - the Netherlands. It is these entities, moreover, that are taking steps to maximise the potential of knowledge of pre-classified CSAM content. In the case of the IWF, the IntelliGrade and IWF Crawler projects (IWF, 2022) should be mentioned, while with regard to its Canadian counterpart, Cybertip!ca, it will be the Arachnid project (Cybertip!ca, 2022). What these projects have in common is the desire to classify as much content as possible in order to make the reference databases of *hash* values as complete as possible.

The use of *hash* values is a solution with many benefits, but this area also needs to be sorted out at international level. This was the aim of a project funded by the European Commission (CNET/LUX/2020/OP/0059, 2021-2022), in which the Dutch organisation EOKM, which also manages the local Meldpunt Kinderporno hotline, took the lead. The aim of this initiative was to lay the foundations for the interoperability of interconnected EU- and global-level sets of *hash* values attributed to CSAM content, which should yield better cooperation between all parties interested in their faster and more efficient removal from cyberspace. The preparation of this paper coincided with the publication of two reports resulting from this project (Publications Office of the European Union, 2022), as well as the start of what appears to be a key undertaking in this field, the Global Standard Project (INHOPE, 2022).

Current situation in Poland

The analysis of current state of undertakings in Poland should begin with a look at how information on CSAM content is managed by national actors dealing with it as part of their duties. These include:

- Dyżurnet.pl;
- the Police;
- representatives of the community of certified specialists and experts;
- representatives of the Internet product and service provider community (private sector).

The diagram below shows the essential elements of the CSAM information management process involving the above-mentioned actors. It is worth pointing out that the current communication between these actors

does not avoid duplication of effort in the research they carry out, resulting in multiple analyses of the same content. Such a practice translates directly into real losses in the state budget, from which the activities of the entities particularly interested in the analyses described here, i.e. law enforcement agencies and the judiciary, are financed.

Dyżurnet.pl is formed by a team of specialists employed at the Research and Academic Computer Network - National Research Institute (hereinafter: NASK), as part of the contact point for reporting illegal content on the Internet, which was established in 2005. As of 2018, the activities of this team were further facilitated by the Act of 5 July 2018 on the National Cyber Security System. Users of cyberspace who have encountered content of concern in this respect can report it in several ways: via the form on the website www.dyzurnet.pl, the e-mail box dyzurnet@dyzurnet.pl, the automated hotline 801 615 005, and, from 2020, also via a plug-in for the Firefox and Chrome browsers.

The content covered by the Dyżurnet.pl response procedure is as follows:

- content depicting the sexual exploitation and abuse of a child: article 202 §3, 4, 4a, 4b of the Act of 6 June 1997, the Penal Code;
- content depicting so-called hard pornography: article 202 §3 of the Penal Code;
- content propagating racism and xenophobia: Article 256 of the Penal Code.;
- other illegal content, i.e. content that does not fall into any of the above categories but endangers the safety of children, e.g. promoting or endorsing paedophilic behaviour (Article 200b of the Penal Code), grooming a minor under 15 years of age via the Internet (Article 200a of the Penal Code), sexual blackmail (also known as sextortion), (Dyżurnet, 2021).

Depending on the location of the server on which the CSAM content is stored, Dyżurnet.pl specialists follow two scenarios. If such content is stored on a server located in Poland or outside Poland, but in a country where an INHOPE-affiliated helpline does not operate, information about it is forwarded to the Police Headquarters in Warsaw, at the following address: cyber-kgp@policja.gov.pl and to INTERPOL. If, however, the reported content is located on a server outside Poland, but in a country where an INHOPE-affiliated helpline operates, it is this helpline and INTERPOL that receive the relevant information. (Dyżurnet.pl, 2021).

In the case of the Dyżurnet.pl operation, INTERPOL is notified, and in practice the images or videos are digitally transmitted to the ICSE DB, through another database, i.e. ICCAM (*I See Child Abuse Material*), launched in 2015 thanks to the cooperation of

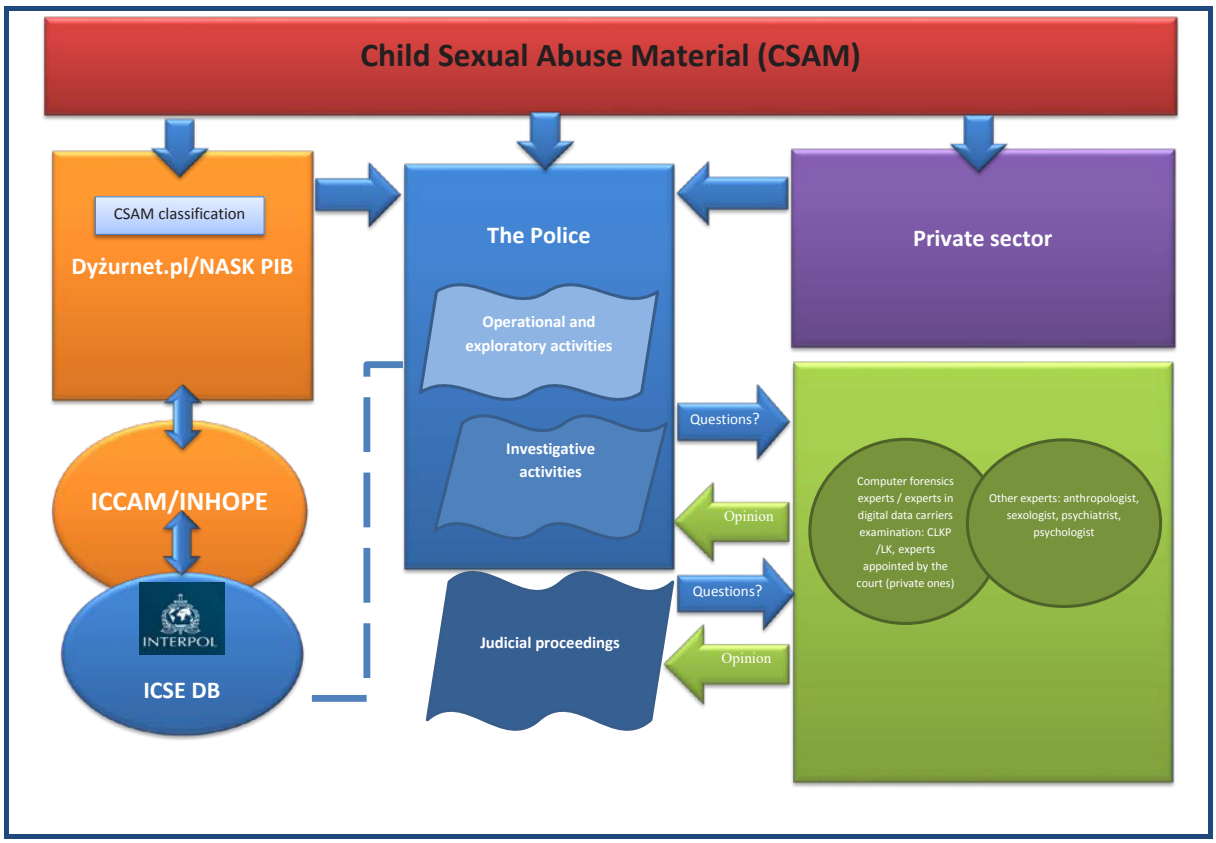

Fig. 1. Diagram concerning the management of information on CSAM in Poland

INHOPE with the private company Ziuz Forensics and EU funding. The most salient feature of this database is the possibility to classify the reported content according to the characteristics of the person pictured on it, such as their gender and approximate age. Based on this classification, content classified as *baseline*, i.e. considered illegal in all INTERPOL cooperating countries, as well as content classified as *national*, i.e. considered illegal in the country of operation of the hotline receiving the call, is submitted to the ICSE DB from the ICCAM database (INHOPE, 2020). The criteria for classifying content in the *baseline* category are as follows: a photo or video should show, without any doubt, an image of a real pre-pubertal child, i.e. before the age of 13, participating in or witnessing sexual activity or should be focused on the genital or anal area of that child (INHOPE, 2021).

If, according to the hotline analyst's initial classification, the content on the reported website can be considered illegal, the URL of such a website is forwarded to the ICCAM database, where an automatic search is performed on all the information at this address, assigning a *hash* value to each photo or video, as well as determining the location of the server. The *hash* value is then compared with lists of other *hash* values that are part of the ICCAM database: content from the *baseline* category and those classified as illegal in both the country of origin of the server and the country receiving the notification. If the *hash* values of newly reported content do not match any of these lists, they are individually classified by the analyst, who assigns them one of three categories: *baseline*, illegal in the analyst's country of work (*national*) or legal in that country. In the case of Poland, Dyżurnet.pl analysts use a distinction between: content defined as 'pornographic content with the participation of a minor' (Article 202 §3, 4, 4a, 4b of the Criminal Code) and 'content presenting a child in a sexual context', such as sexually oriented posing.

The Polish Police is another entity that deals with CSAM content as part of their duties. This applies to various areas of their activities and related powers: operational and exploratory activities, investigative activities, as well as participation in court proceedings. However, the overriding problem of this formation is the limited - in comparison to many other, foreign police formations - use of powers to identify child victims of sexual exploitation and/or abuse. Such identification is aimed at determining, first, the identity and location of a child whose image has been recorded in materials containing a visual recording of a criminal act with his/her participation, and second, a potential perpetrator of sexual exploitation and/or abuse. The main reason for such a situation is the lack of a systemic approach to the verification of such materials, which boils down to access to a key tool in this area, i.e. the ICSE DB, only at the national level, through the Police Headquarters in Warsaw (the Department for Combating Trafficking in Human Beings located within the structures of the Crime Bureau). Other reasons for this can be attributed to the inability to use other tools described here: a central reference database containing files in CSAM category, as well as to not having its own reliable list of *hash* values relating to material that has previously been classified as CSAM by police officers coming into contact with it in the course of their official duties. A 'reliable' list of *hash* values should be understood as a list produced as a result of a process based on a uniform CSAM classification system, taking into account the experience resulting from the exchange of information and training taking place especially at international level. The principle often applied here is that the classification given to CSAM files should be verified by three people in order to obtain full agreement in their assessment.

In addition, there are certified specialists[2] and experts[3], with specialisations in computer forensics and examination of digital data carriers, employed in the police forensic laboratories, who may also - within the framework of orders and decisions received - come into contact with content from CSAM category (Central Forensic Laboratory of the Police, 2018). Unfortunately, documents in the form of methodologies for computer and digital data carrier examination are not generally available, so issues in this area could not be included in this study. This is undoubtedly a topic for a separate publication involving representatives of this community. However, it will be useful here to refer to the scopes of activities of certified specialists and experts employed in laboratories dealing with digital data carriers and computers, published e.g. by the Forensic Laboratory of the Voivodeship Police Headquarters in Łódź. According to these, the scope of activities of a certified specialist employed in the laboratory dealing with digital data carriers includes the following:

- making image copies from visual records;
- recording of procedural acts;
- extracting frames from visual records and their editing;
- preparing demonstrative documentation;
- securing data from digital data carriers;
- making binary copies of digital data carriers;
- reading the contents of mobile phones;
- viewing, pre-selecting and converting files;
- securing records from digital video recorders.

As far as the scope of activities of an expert from the same laboratory is concerned, in addition to the

[2] The title of certified specialist entitles the holder to carry out independent technical activities, documented - in terms of their conduct and results - in a report.

[3] The title of expert, on the other hand, entitles one to independently carry out technical activities, examinations, as well as to make conclusions (art. 200 §2 item 5, Act of 6 June 1997, Code of Criminal Procedure), documented in a prepared opinion, which has a legal basis in, inter alia, art. 193 of the Code of Criminal Procedure.

above-mentioned activities, it also includes the following:

- identification of recorded objects, facilities and places based on visual records (clothing, vehicles, identification numbers/plate numbers, logos);
- identification of recording devices;
- examination of visual records to identify methods and traces of tampering with the recorded image;
- research aimed at determining facility sizes based on the recorded image;
- making other determinations possible on the basis of the analysis of visual records (e.g. selection of material, determination of the time of image recording, place of recording, equipment used for recording), (Forensic Laboratory of the Voivodeship Police Headquarters in Łódź, 2022).

In the case of the Computer Forensics Laboratory, the typical scope of activities of a certified specialist includes the following:

- securing data from computers, disks;
- making copies of data carriers;
- downloading the contents of mobile phones;
- viewing files and their pre-selection;
- file conversion.

In contrast, an expert employed in the same laboratory, in addition to the above-mentioned activities, will also:

- examine computer hardware and peripheral hardware;
- determine the purpose of computing devices, their performance and the content of their memory;
- determine and analyse the content of digital data carriers with the exception of:
  - establishing the legality, value and copyright holders of programmes, audio and video files and the content of text files,
  - determine the gender and age of the persons recorded in the files and the nature of their content (e.g.: pornography, erotica, violence, etc.),
- recover data from digital data carriers and analyse them, with the exceptions mentioned in item 3;
- examine GSM phones - read data from memory and SIM cards, (Forensic Laboratory of the Voivodeship Police Headquarters in Łódź, 2022).

It is easy to see that the activities described above are directed at two areas: the content of digital data carriers and the activity of their user, while their aim is to provide an expert's opinion on information relevant to the proceedings. In this case, the key observation for the issues analysed in this paper, concerning this group of police officers and employees, will be that their activities are therefore conducted from a completely different angle than the identification of a child and a perpetrator of a sexual offence committed against the child. According to their scopes of work, certified specialists and experts should not comment on the sex and age of the persons recorded in the files and the nature of file content, which in turn is the basis of any identification operation. On the other hand, it seems that, by virtue of their skills, these persons could lay the foundations of a new forensic specialisation dealing with the issues of victim or perpetrator identification, or cooperate with an interdisciplinary team established, for example at central level, to carry out activities in this area.

Problems affecting this professional group, which need to be resolved as a matter of priority, also include the lack of communication between laboratories, resulting in the possibility of situations where files with the same content are dealt with by unaware police officers in neighbouring units.

Restrictions of a similar nature also apply to other experts who give opinions on potentially illegal content at the request of the prosecutor's office or court. As a rule, these experts' competences are interdisciplinary and they perform their duties as experts on an ancillary basis. In addition, differences in competence between experts of different specialisations often require complementary analyses: an example of this is the cooperation of an expert sexologist and anthropologist to assess the age of a child depicted in the analysed content (comprehensive opinion). The process of assessing the content on which these experts are to comment is usually time-consuming and, in most cases, dependent on the type of audiovisual material, i.e. photos vs. videos, as well as its quantity and content. At present, a major impediment to work of these experts is the lack of standards unifying their work, especially on such key issues as the approach to the content to be assessed, i.e. each image individually vs. an overall assessment of content of a certain nature, access to training or the need for them to have visual records which may contain illegal content on their own computer equipment.

The last group of entities included in the diagram are the so-called private sector entities, comprising providers of various types of Internet products and services. It is difficult to draw the real picture of the engagement of these providers (both domestic and foreign ones), operating in Poland, in counteracting the availability of CSAM in their products and services. First of all, there is no legal requirement in Poland, as there is in the United States, for these providers to send the Dyżurnet.pl team reports on potential CSAM incidents. However, this state of affairs is likely to change significantly in the near future thanks to EU-level initiatives dedicated to this area. In July 2020, an EU strategy calling for a more effective fight against child sexual abuse was announced (European Commission, 2020), followed shortly thereafter by a new legislative proposal in the form of a Digital Services Act (European Commission, 2020) in December 2020. For the field discussed here, however, the solutions accompanying the European Commission's next legislative proposal, in May 2022, regulating the obligations of ISPs in the area of detection, reporting and removal of CSAM from their

products and services (European Commission, 2022), will be crucial. It is worth noting at this point that, almost as soon as it was announced, a global discussion began regarding the need to draw a line between measures to protect children and the privacy rights of users of these products and services.

Proposals for solutions to improve the current situation at national level

Taking into account the considerations presented in the earlier parts of this study, it should be assumed that, in the case of Poland, a significant improvement of the current situation can be achieved through the implementation of systemic solutions, within which the aforementioned entities will be able to use technological solutions available on the market. Such an approach has long been promoted by experts in the field under discussion (e.g. WeProtect, 2021).

Systemic solutions presented later in this paper at national level involve a two-pronged approach, consisting of:

- treating the the CSAM content available in cyberspace as evidence of a crime and giving it the right priority to reach child victims of real-time sexual exploitation and/or abuse first (the role of law enforcement authorities), and
- removing such content, even historical one, from cyberspace (the role of Dyżurnet.pl and the private sector).

The systemic changes advocated here, as shown in the diagram below, are therefore based on the implementation of relevant tools at national level: National CSAM Database, i.e. a database of audiovisual material depicting child sexual abuse, and lists containing *hash* values attributed to content classified as CSAM in a reliable process. A key element of these changes should be considered the enabling of communication between operating entities accessing the CSAM as part of their duties. Such functionality is offered, for example, by a solution in the form of the *Hash Check Service* (hereinafter: HCS), which has been implemented since 2019 in the Netherlands and is currently being transformed into a more advanced form, referred to as *Instant Image Identifier* (EOKM, 2022). In a nutshell, this solution allows authorised entities to send a query as to whether a file in their possession is a previously classified CSAM. This communication, using the web protocol HTTPS, takes place without the need to send the actual file - the *hash* value assigned to it is compared, via a dedicated API interface, with the contents of a set of such values managed by the Dutch organisation EOKM, already mentioned here. Depending on the results of the check, the submitter of the request receives a 'yes' or 'no' response.

The solutions proposed here include, in the first place, the Police, whose resources should include the National CSAM Database, enabling communication with field units of this formation, where materials secured in connection with proceedings conducted in Poland would be delivered. The key argument against the allegation that this would be a duplication of the ICSE database is the possibility for the Police to create their own list of *hash* values, extended each time when new content in this category is revealed and classified as part of their operations. Such activities would have a direct impact on increasing the efficiency of the service in the area discussed here. In addition, the competence to identify child victims of sexual exploitation and abuse should include specially appointed teams in police field units, carrying out operational, exploratory and investigative activities, hence the change postulated in this area is to allow access to the ICSE DB to police field units, i.e. at the level of each voivodeship, including the Warsaw Metropolitan Police.

The police list of *hash* values (only the list, not the actual files or their copies) would be made available to NASK, and in practice to the Dyżurnet.pl team, responsible for the functioning of HCS in Polish conditions. Dyżurnet.pl's task would be to manage the collected lists: its own, which would include digital signatures of files of which the Dyżurnet.pl team has been notified via dedicated channels or in cooperation with the private sector, the police list, as well as lists obtained from reliable partners such as INTERPOL, Europol, NCMEC or IWF. It is worth mentioning that similar efforts in this area have been made in the past by NASK, with the launch of the SYWENTO application. It supports the analysis of data by computer forensics experts to obtain information on whether a given Internet address (URL) contains pornographic content with a minor. A query sent to the SYWENTO application generates feedback as to whether the URLs entered into the system by the expert are present in the database of addresses identified by Dyżurnet.pl. (Dyżurnet.pl, 2022).

In addition to equipping police officers with technological tools, persons serving in teams dedicated to combating child sexual exploitation and abuse should receive mandatory, specialised training, covering the characteristics of this phenomenon, techniques for interviewing perpetrators and victims, as well as how to deal with the consequences of contact with such a specific type of crime, including the need to classify CSAM. It also seems reasonable to enrich the range of competences of police psychologists so that they can provide systemic and proactive assistance to their colleagues confronted in their work with one of the most difficult challenges of dealing with child sexual abuse material.

The possibility to submit queries to the HCS would be particularly helpful for private sector entities in Poland, which could thus verify the content of their products and services without incurring the costs associated with the individual implementation of such solutions, including the hiring and training of content moderators. In view of the changes to be brought about by the

package of EU legislative proposals in this area, such a service should be of particular interest to small and medium-sized private sector entities, for which compliance with the new regulations may constitute a significant financial burden.

The group of entities that could benefit from the functioning of the HCS would also include experts operating outside the police, for whom the possibility of making queries would contribute to increasing the efficiency of their work, as well as giving it some form of standardisation.

Summary

Cyberspace is now a place where children are groomed, solicitated and even blackmailed into obtaining sexually explicit content involving them, which translates directly into an alarming amount of such content available in this dimension. Europol representatives speak directly about the serious consequences of the increasing amount of CSAM revealed in cyberspace, year after year, for the capabilities of law enforcement agencies worldwide to identify perpetrators (Europol, 2020). In the face of such challenges, calls for the use of available technologies are therefore particularly timely.

Some efforts to change the current situation in Poland were made within the framework of a project of the Police Headquarters and the Central Forensic Laboratory of the Police called "Development of a Central Information System for Files Related to Criminal Activity", financed from 2014 to 2020 under the EU Internal Security Fund (Police, 2020), the aim of which was to develop an integrated, central system of information on files (*hashes*) related to criminal activity, called the Central Hash System. Detailed information on this subject is held by Central Forensic Laboratory of the Police, as an institution exercising substantive supervision over the project. It should be assumed that the experience gained within the framework of this project will allow for the implementation of systemic solutions postulated in this study at national level. Undoubtedly, a key element in this case will be the compatibility of the system used in this project for classifying files related to criminal activity with the system used in practice by specialists employed in Dyżurnet.pl, who are trained, among others, by INTERPOL.

Another opportunity to change the national situation was when NASK submitted a proposal for the NETTO (*Networking Enhanced Through Technological Opportunities*) project in February 2021, worth approximately

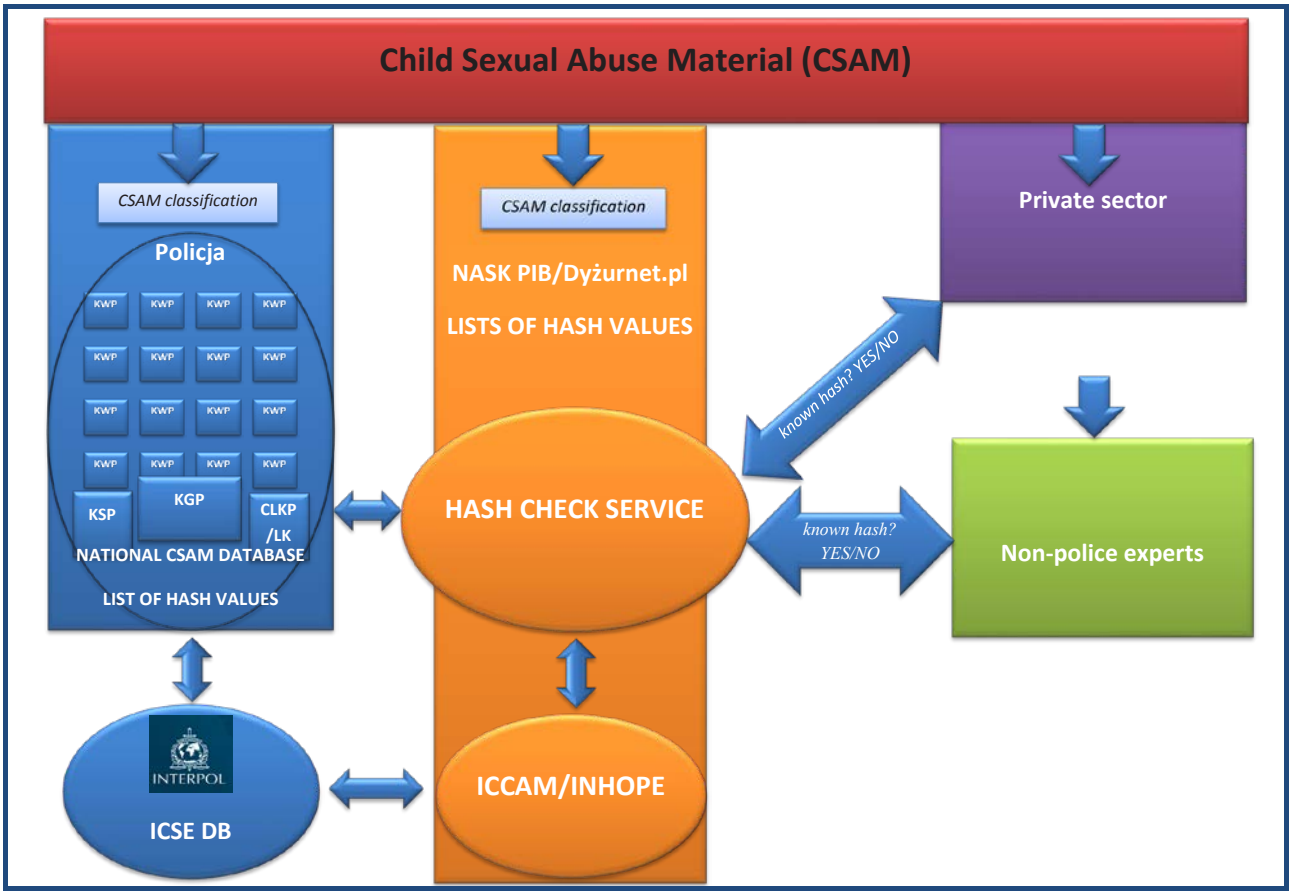

Fig. 2. Proposal to implement *hash* value exchange solutions in Poland

€1 million, under the EU's Internal Security Fund. This proposal, despite receiving a high score in the project competition, did not ultimately receive funding, which did not prejudge the re-use of the concept contained therein in another NASK project submitted to the competition a year later.

The hope for a change in the national response to the problem of child sexual exploitation and abuse can now be pinned on two recent initiatives that are significant for the area discussed here. The first one is the appointment, by Order of the Minister of Justice of 29 September 2021, of a Team for counteracting crimes against sexual freedom and morality committed to the detriment of minors (Ministry of Justice, 2021). The second initiative is the establishment of the Central Cybercrime Bureau in the Police, as of 12 January 2022 (Police, 2021). Here, it seems crucial to assume that the phenomenon of child sexual exploitation and abuse in cyberspace falls under the category of cybercrime. This assumption should be reflected in the decisions defining the organisation and competences of the newly established Bureau.

Source of figures: author

Bibliography

1. Canadian Centre for Child Protection, (2017). Survivors' survey. (Accessed on 27/01/22: https://www.protectchildren.ca/en/resources-research/survivors-survey-results/).
2. Central Forensic Laboratory of the Police, (2017). Computer forensics. (Accessed on 21/03/2022: https://clkp.policja.pl/clk/badania-i-projekty/langnodata/badania-informatyczne/153011,Badania-Informatyczne.html).
3. Central Forensic Laboratory of the Police, (2017). Decision No. 164 of the Director of Central Forensic Laboratory of the Police of 29.06.2018 on the list of forensic specialities within the scope of which opinions and reports on activities carried out in police forensic laboratories are issued.
4. Central Forensic Laboratory of the Police, (2018). Decision No. 164 of the Director of Central Forensic Laboratory of the Police of 29.06.2018 on typical scopes of work of an expert and specialist in forensic specialties.
5. Child Rescue Coalition, (2021). (Accessed on 11/10/21: https://childrescuecoalition.org/the-issue/).
6. Cybertip!ca, (2022). (Accessed on 30/05/2022: https://www.cybertip.ca/en/child-sexual-abuse/project-arachnid/).
7. Dyżurnet.pl, (2021). Report by Dyżurnet.pl 2020. (Accessed on: 11/10/21: https://dyzurnet.pl/publikacje).
8. Dyżurnet.pl, (2022). (Accessed on 30/05/2022: https://dyzurnet.pl/dla-profesjonalistow/wpis/sywento).
9. Elshenraki, H.N. (2021), Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities. *Advances in Criminology, Criminal Justice, and Penology.*
10. EOKM, (2022). (Accessed on 30/05/2022: https://www.3-is.eu/#objectives andhttps://www.3-is.eu/sites/default/files/2022-05/iii-description-tool-v2_0.pdf).
11. Europol, (2015). (Accessed on 16/05/22: https://www.europol.europa.eu/sites/default/files/documents/efc_strategic_assessment__public_version.pdf).
12. Europol, (2017). (Accessed on 11/10/21: https://www.europol.europa.eu/newsroom/news/14-arrests-in-takedown-of-massive-child-sexual-abuse-platform andhttps://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe).
13. Europol, (2020). Internet Organised Crime Threat Assessment. (Accessed on 11/10/21: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020).
14. Europol, (2021). Internet Organised Crime Threat Assessment. (Accessed on 03/02/2022: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021).
15. Gazeta Policyjna, (2021). Numer 2 Specjalny. (Accessed on 27/01/2022: https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s).
16. INHOPE, (2020). Annual report 2020. (Accessed on 12/10/21: https://inhope.org/media/pages/the-facts/download-our-whitepapers/annual-report/bb4dd3cdc3-1628156678/inhope-annual-report-2020.pdf).
17. INHOPE, (2021). (Accessed on 11/10/21: https://www.inhope.org/EN, https://inhope.org/EN/articles/what-is-baseline).
18. INHOPE, (2022). Accessed on 21/11/22: https://inhope.org/EN/articles/the-global-standard-project.
19. Internet Watch Foundation, (2022). (Accessed on 30/05/22: https://www.iwf.org.uk/our-technology/intelligrade/ and https://www.iwf.org.uk/our-technology/crawler/).
20. INTERPOL, (2022). (Accessed on 21/11/22: https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database).
21. European Commission, (2020). 'EU strategy for a more effective fight against child sexual abuse'. (Accessed on: 03/02/2022: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agendasecurity/20200724_com-2020-607-commission-communication_en.pdf).
22. European Commission, (2020). Networks, Content and Technology, *Study on framework of best practices to tackle child sexual abuse material online: executive summary (English)*, Publications Office, 2020, https://data.europa.eu/doi/10.2759/386477.

23. European Commission, (2020). Digital Services Act. (Accessed on: 03/02/2022: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_pl).
24. European Commission, (2022). (Accessed on: 30/05/22: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472).
25. Forensic Laboratory of Voivodeship Police Headquarters in Łódź. (Accessed on: 11/07/22: https://lk-lodzka.policja.gov.pl/el8/struktura/sekcja-dokumentow/pracownia-cyfrowych-nos/606,Pracownia-Cyfrowych-Nosnikow-Danych.html and https://lk-lodzka.policja.gov.pl/el8/struktura/sekcja-dokumentow/pracownia-badan-informa/604,Pracownia-Badan-Informatycznych.html).
26. Lee, H-E., Ermakova, T., Ververis, V., Fabian, B. (2020). Detecting child abuse material: A comprehensive survey. Forensic Science International: Digital Investigation, *34*. http://doi.org/10.1016/j.fsidi.2020.301022.
27. Microsoft, (2020). (Accessed on 21/11/2022: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/).
28. National Center for Missing & Exploited Children, (2020). (Accessed on 08/09/2021: https://www.missingkids.org/gethelpnow/cybertipline).
29. National Center for Missing & Exploited Children, (2020). (Accessed on 28/04/2022: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata).
30. Police, (2020). (Accessed on 08/09/2021: https://clkp.policja.pl/clk/badania-i-projekty/fundusz-bezpieczenstwa/153261,Fundusz-Bezpieczenstwa-Wewnetrznego.html).
31. Publications Office of the European Union, (2022). (Accessed on 14/06/22: https://op.europa.eu/en/publication-detail/-/publication/986ca706-cce4-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257046699 and https://op.europa.eu/en/publication-detail/-/publication/3e8e564c-cce7-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257046650).
32. Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum, 21*, 429-447. http://doi.org/10.1007/s12027-020-00625-7.
33. Council of Europe, (2021). Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse. (Accessed on 11/10/21), https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee).
34. Seto, M.C., Hanson, R.K., Babchishin, K.C. (2010). Contact Sexual Offending by Men With Online Sexual Offenses. *Sexual Abuse: A Journal of Research and Treatment*, *23*(1), 124-145. http://doi.org/10.1177/1079063210369013.
35. Act of 5 July 2018, on the National Cyber Security System (Journal of Laws 2020, item 1369, as amended).
36. Act of 6 June 1997, Penal Code (Journal of Laws 2021, item 2345, as amended).
37. Act of 6 June 1997, Code of Criminal Procedure (Journal of Laws 2021, item 534 as amended).
38. Act of 17 December 2021, amending certain acts in connection with the establishment of the Central Cybercrime Bureau (Journal of Laws 2021, item 2447).
39. Wasilewski, J. (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego*, *9*, 225-234.
40. WeProtect, (2021). The Model National Response. (Accessed on 03/02/2022: https://www.weprotect.org/model-national-response/).
41. Web-IQ, (2020). EU Strategy proposal CSAM lifecycle and interception. (Accessed on 08/09/2021: https://vimeo.com/434684287).
42. Order of the Minister of Justice of 29 September 2021 on the appointment of a Team for counteracting crimes against sexual freedom and morality to the detriment of minors. (Accessed on 03/02/2022: https://www.gov.pl/web/sprawiedliwosc/du-21-233).

Translation GTC AMG sp. z o.o.