2021 REPORT

dyżurnet.pl
NASK

CSIRT NASK

EDITOR

NASK National Research Institute

Kolska 12 St.
01-045 Warsaw
e-mail: info@nask.pl, info@dyzurnet.pl

issn 2084-7785

Text: Dyżurnet.pl team

Correction: Anna Hernik-Solarska

graphic design and illustrations: Agnieszka Malinowska

dyżurnet.pl
NASK

INHOPE

saferinternet.pl

Co-financed by the European Union
Connecting Europe Facility

WE ACT

to develop a secure internet

WE REACT

to illegal and harmful online content addressed against the safety of children and teenagers

WE POPULARISE

secure use of the Internet

dyżurnet.pl

NASK

INTRODUCTION

Ladies and Gentlemen,

The report on the activities of the Dyżurnet.pl Team is an opportunity to reflect on threats that occur on the Internet and are related to new technologies. For NASK PIB, activities aimed at increasing Internet or technological safety have always been important, and the establishment of the Dyżurnet.pl team in 2005 showed that counteracting child sexual abuse material is a necessary step. Since 2018, the activity of Dyżurnet.pl has been included in the Act on the National Cyber Security System, and the Team performs the tasks of CSIRT NASK.

The Team's uniqueness lies in the fact that it analyzes content that is not widely available and links users, online platforms, law enforcement agencies or government institutions. Our perspective allows us to analyze phenomena that may be elusive to others. From our point of view, the alarming message drawing attention to sexual content self-generated by children is significant in this year's report. Independent does not mean voluntary. The child does not have enough experience and knowledge to understand the whole context of the situation. Therefore, it is necessary to support all individuals and institutions to prevent the creation of intimate content and to counteract as effectively as possible the effects of the distribution of images or films depicting the sexual abuse of the youngest.

We hope that the report showing the scale of the phenomena related to online abuse, illegal and inappropriate content and containing descriptions of our activities will inspire you to think about the challenges posed by the digital world. Let's be in it together because only then is it possible to take care of the youngest users of cyberspace.

Sincerely,
Krzysztof Silicki
Director of Cybersecurity and Innovation at NASK

TABLE OF CONTENTS

ABOUT US

we act - we react - we promote

The Dyżurnet.pl team was established in 2005 at NASK. It is the only team in Poland responding to illegal and harmful content on the Internet. In addition, as part of its activities under the National Cyber Security System Act, it accepts child sexual abuse material reports.

Since its inception, Dyżurnet.pl has been a member of INHOPE Association https://inhope.org/ - a global network of response teams from different countries, cooperating with international law enforcement agencies, e.g. Interpol and Internet companies.
The Association's goal is to support national hotlines against the distribution of child sexual abuse material.

Since 2005, the Dyżurnet.pl team has been implementing the European Commission's Better Internet for Children strategy, co-creating **Polish Safer Internet Program Center (PCPSI)** https://www.saferinternet.pl/. It is created by NASK National Research Institute (PCPSI coordinator) and the "Empowering Children" (Dajemy Dzieciom Siłę) Foundation. The strategy, implemented in most European countries (www.betterinterntetforkids.eu), aims to promote safer use of the Internet and new technologies and to support the response to online risks affecting the youngest.

helpline:
116 111
800 100 100

HOW DO WE WORK?

Dyżurnet.pl accepts reports through:

- www.dyzurnet.pl website form
- email address dyzurnet@dyzurnet.pl
- an automated hotline at 801 615 005.
- google Chrome browser plug-in: Report illegal content to Dyżurnet.pl
- mozilla Firefox browser plug-in: Submit content to Dyżurnet.pl

Due to the harmfulness and possible criminal consequences of accessing illegal content, the Dyżurnet.pl team advises against searching for such content on the Internet on your own.

Categories that are included in the response procedure*:

- Material depicting the sexual abuse of a child: art. 202 §3, 4, 4a, 4b of the Penal Code - Polish law prohibits the production, recording, import, distribution, presentation, storage, access and possession of pornographic content with the participation of a minor;

- Materials depicting hard pornography: article 202 §3 of the Penal Code - Polish law prohibits the dissemination and public presentation of pornography involving the use of violence or the use of an animal;

- Content propagating racism and xenophobia: Article 256 of the Penal Code - Polish law prohibits the propagation of fascist or other totalitarian state systems and incitement to hatred on the grounds of national, ethnic, racial, religious differences or on the grounds of irreligiousness;

- Other illegal content: content that does not fall under any of the above categories but is directed against the safety of children, e.g. advocating or praising paedophilic behaviour (Article 200b of the Penal Code), online grooming of a child under 15 years of age (Article 200a of the Penal Code), sexual blackmail (also known as sextortion).

Child sexual abuse content is the most important group of reports submitted by Internet users to the Dyżurnet.pl team.

* Articles of the Penal Code in incomplete form

Depending on the classification of the request and the location of the server where the submitted content is stored, the Team takes the following actions according to the procedure:

- if the child sexual abuse material is located on a server located in Poland, the information is forwarded to the Police Headquarters and Interpol;
- if the child sexual abuse material is located on a server in a country covered by the INHOPE Association, this information is forwarded to the response team responsible for the country of the server's location and to Interpol;
- if the child sexual abuse material is located on a server outside the reach of INHOPE, this information is forwarded to Police Headquarters and Interpol.

All materials (photos and videos) depicting child sexual abuse are submitted to the ICCAM database for the identification of victims and perpetrators.

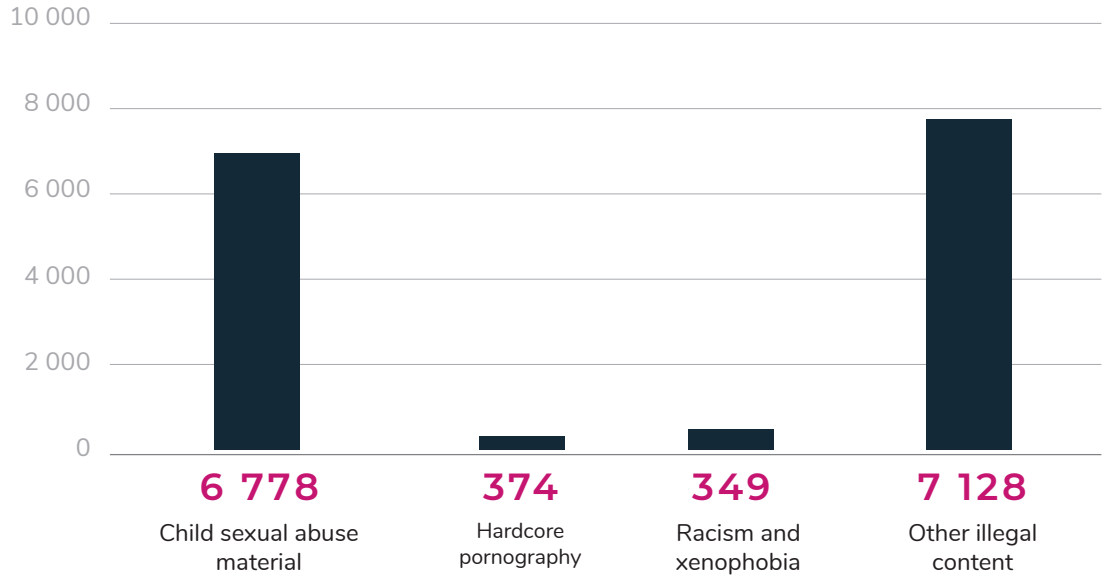
The efforts of all response teams and cooperating law enforcement agencies are to identify the perpetrator and victim of sexual abuse as quickly as possible. Reporting by the user and prompt action by an administrator can significantly reduce further disseminating of child sexual abuse material.

STATISTICS

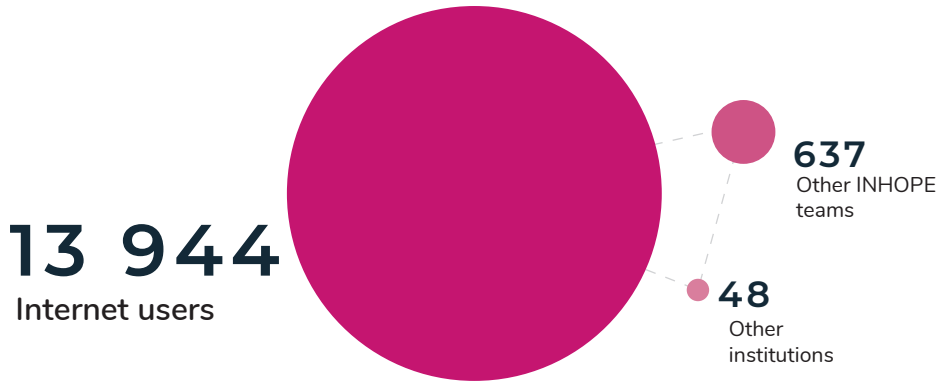
Dyżurnet.pl for 2021

Reports received by Dyżurnet.pl team

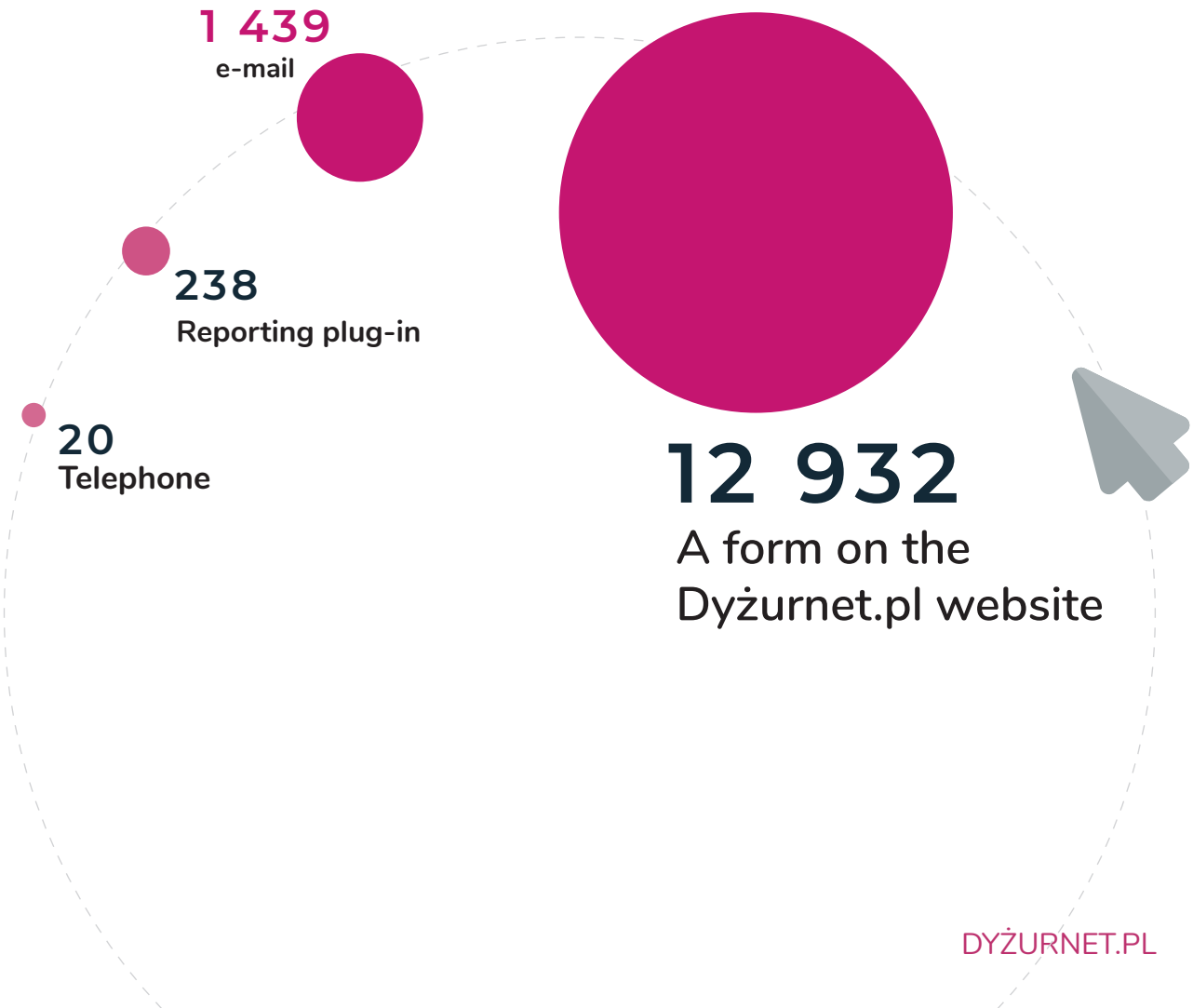
1 | Number of reports received by Dyżurnet.pl - type of potentially illegal content



2 | Number of reports received by Dyżurnet.pl - type of applicant



3 | Number of reports received by Dyżurnet.pl - report source



Incidents analysed and actions taken by Dyżurnet.pl team

4 | Classification of incidents involving the sexual exploitation of minors

2069

CSAM

CSAM (child sexual abuse materials)
Child sexual abuse content. Under Polish law it is illegal; defined as pornographic content with the participation of a minor (art. 202 § 3, 4, 4a, 4b of the Penal Code).

409

CSEM

CSEM (child sexual exploitation materials)
Content that presents a child in a sexual context, not qualifying as CSAM. Includes so-called “modelling" and "sexual posing."

18

Propagation of pedophilic activity

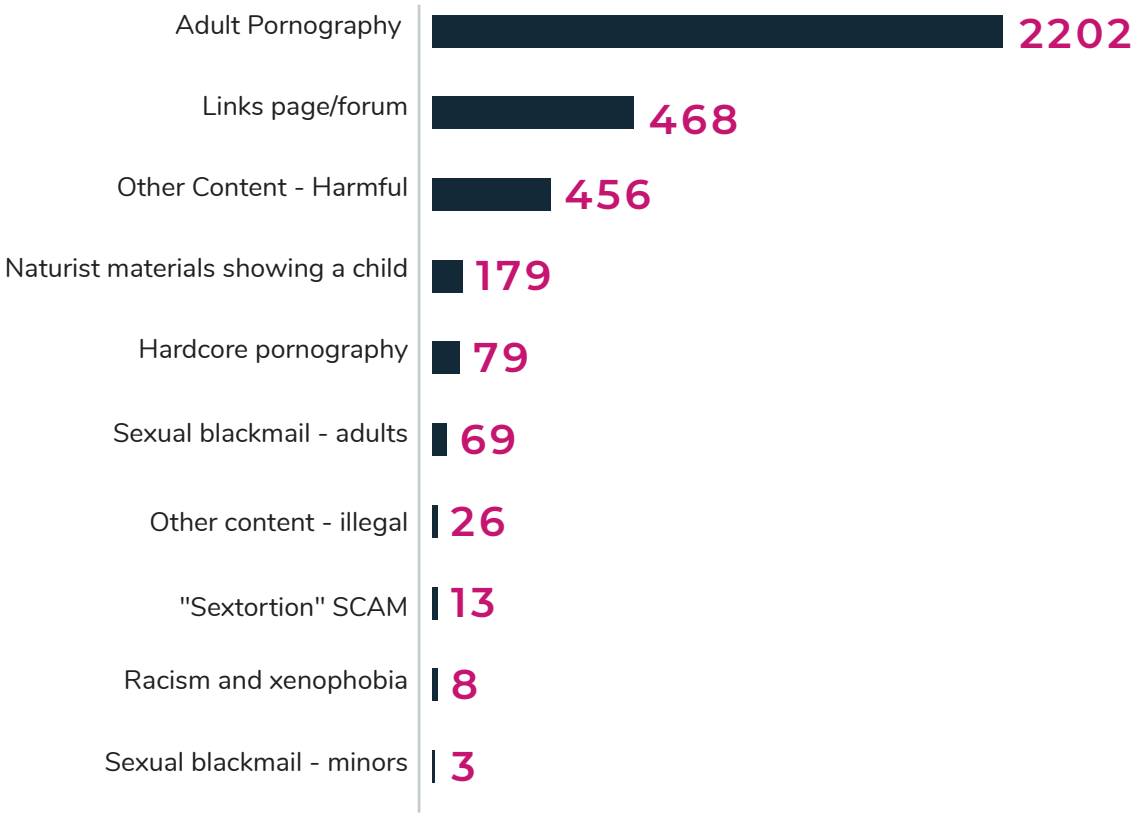
Propagation of pedophilic activity
Public promotion or praising of paedophilic behaviour; illegal according to Polish law (Article 200b of the Penal Code).

10

Child grooming

Child grooming
Contact with a minor under the age of 15 for sexual intercourse, submission to or performance of other sexual act, or participation in the roduction or recording of pornographic content; illegal under Polish law (Article 200a of the Penal Code).

5 | Classification of incidents involving other illegal and harmful content



Adult Pornography
Pornographic content involving persons appearing to be of legal age.

Links page/forum
Web sites or forums that contain only links to external resources.

Other Content - Harmful
Content harmful to persons under 18 and eligible for blocking in the OSE network: drastic content, vulgar, offensive, radical worldview (including sects), homophobic, self-destructive, promoting suicide or violence, pro-ana, pathostreams, psychoactive substances (not explicitly identified as drugs).

Naturist content with a child
Content that presents naked children without intentional sexual context, usually nudist or naturist content of a neutral nature.

Hardcore pornography
Pornographic content with the participation of persons appearing to be adults, containing scenes involving the depiction of violence or the use of an animal; illegal under Polish law (Art. 202 § 3 of the Penal Code).

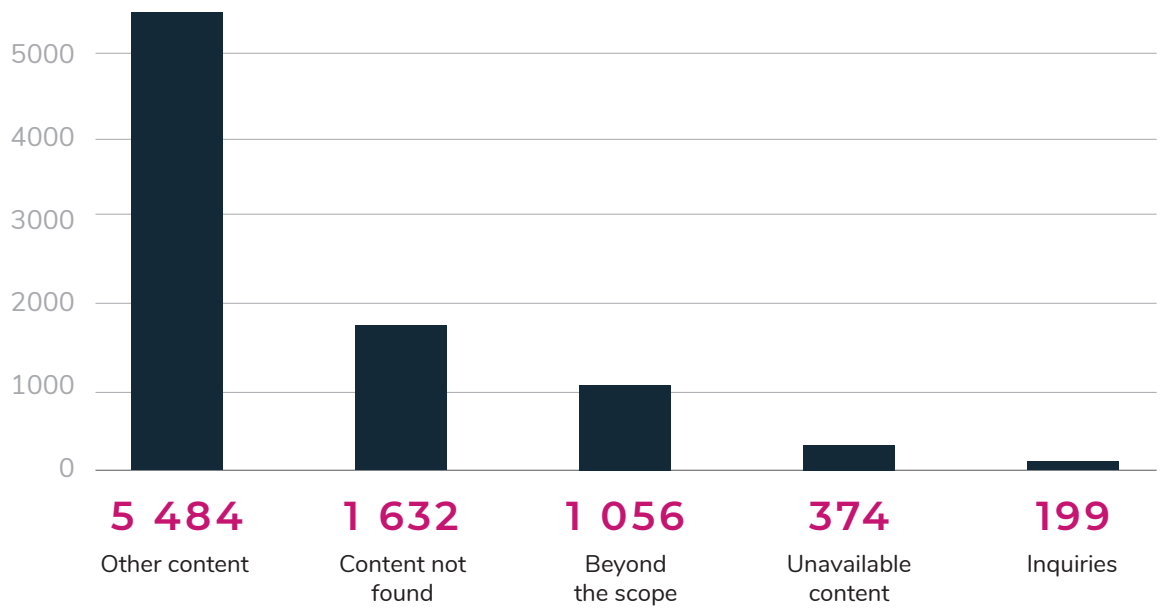
Sexual blackmail ("sextortion")
Sexual extortion, blackmail involving obtaining sexually explicit multimedia material from the victim under threat of making it more widely available; may involve obtaining material benefits. The classification is broken down into adult and juvenile cases.

Other content - illegal
Content penalized by the Polish Penal Code and threatening children's safety, included in the scope of Dyżurnet.pl team's response.

Sextortion scam
Bulk mailings of allegedly obtained sexually explicit material involving the recipient; one form of phishing targeting individuals who have been victims of a log-in data leak.

Racism and xenophobia
Content publicly propagating a totalitarian state system, inciting hatred and insulting due to national, ethnic, racial, religious affiliation or irreligiousness; illegal under Polish law (Articles 256 and 257 of the Penal Code).

6 | Classification of other incident categories



Other content
Content outside of the listed categories that is not harmful or illegal content.

Content not found
When Dyżurnet.pl investigated the report, the content in question was not found, and most likely had already been removed.

Beyond the scope
Cases involving violations of law, but beyond the scope of intervention of Dyżurnet.pl: defamation, insults, stalking, threats, violation of personal rights and image, cases related to personal data (phishing, sharing without permission), phishing and financial fraud (including fake online stores), account hacking and data theft, copyright infringement, gambling, distribution of pharmaceuticals outside of pharmacies, information about the availability of treatments or abortions, publication of potentially false information, false profiles of institutions, false documents.

Unavailable content
Password-protected content, downloads located on servers outside of Poland and sites identified as effectively masking their content.

Inquiries
Questions from Internet users and other institutions about illegal and harmful content published online.

7 | Actions taken by Dyżurnet.pl against all categories of incidents

1 975
Reported to the relevant INHOPE team and Interpol

281
Reported to the service administrators

51
Reported to the ISP

12
Reported to the content owner

107
Forwarded to another entity (mainly CERT Polska)

145
Reported to the Police

Reported to the relevant INHOPE team and Interpol
The baseline content (material that constitutes illegal content in all INHOPE countries) submitted via the ICCAM database or contact form to the response teams appropriate to the server location, affiliated with the INHOPE Association is submitted to ICSE (International Child Sexual Exploitation Database) at Interpol.

Reported to service administrators
A report sent to an Internet service's administrators or moderation department concerning content that is not illegal but does not comply with the terms of service.

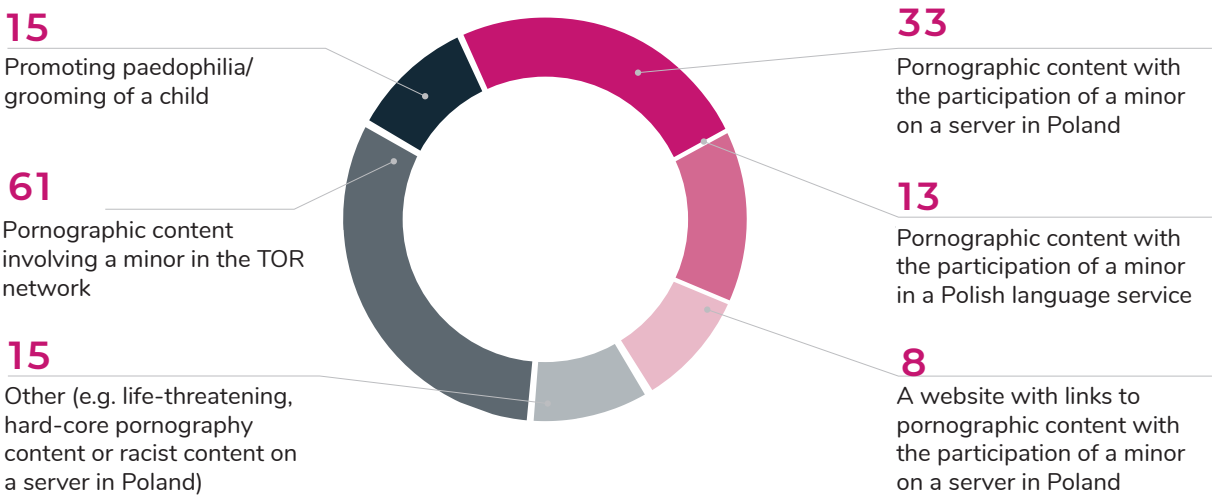
Reported to the ISP
Sending a notice of unlawful content (relating to CSAM) following Article 14 of the Law on Provision of Electronic Services in the case of a hosting provider in Poland or informing a hosting provider located outside INHOPE's reach of unlawful content (relating to CSAM) located on its servers.

Reported to content owner
Reports regarding harmful content to the author of the content for consideration of an appropriate warning or removal.

Transferred to another entity
Forwarded to cooperating institutions in accordance with their scope of activity (mainly CERT Polska within CSIRT NASK and "Dajemy Dzieciom Siłę" Foundation).

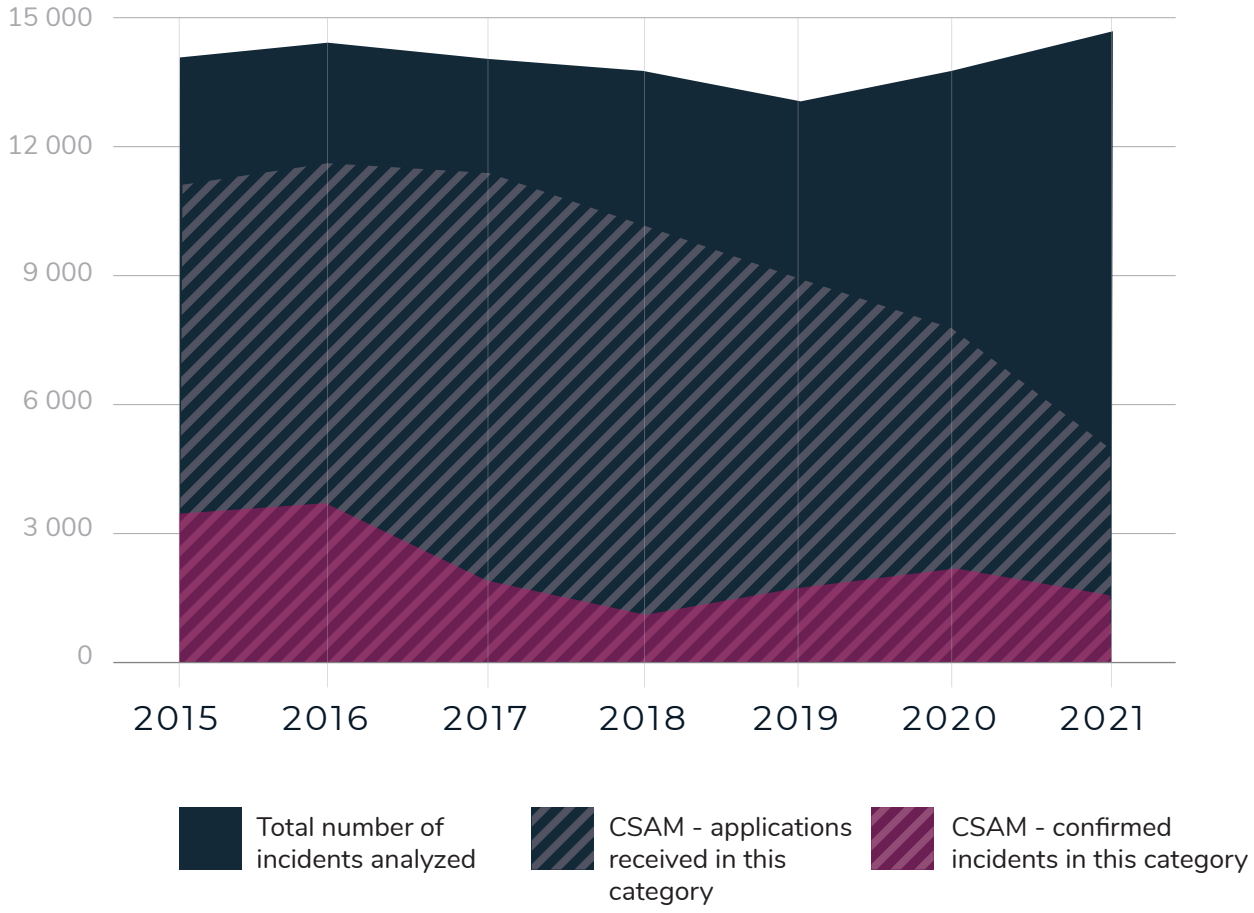
Reported to the Police
Forwarded to the Cybercrime Bureau of the Police Headquarters.

8 | Reports sent to the Cybercrime Bureau of the National Police Headquarters



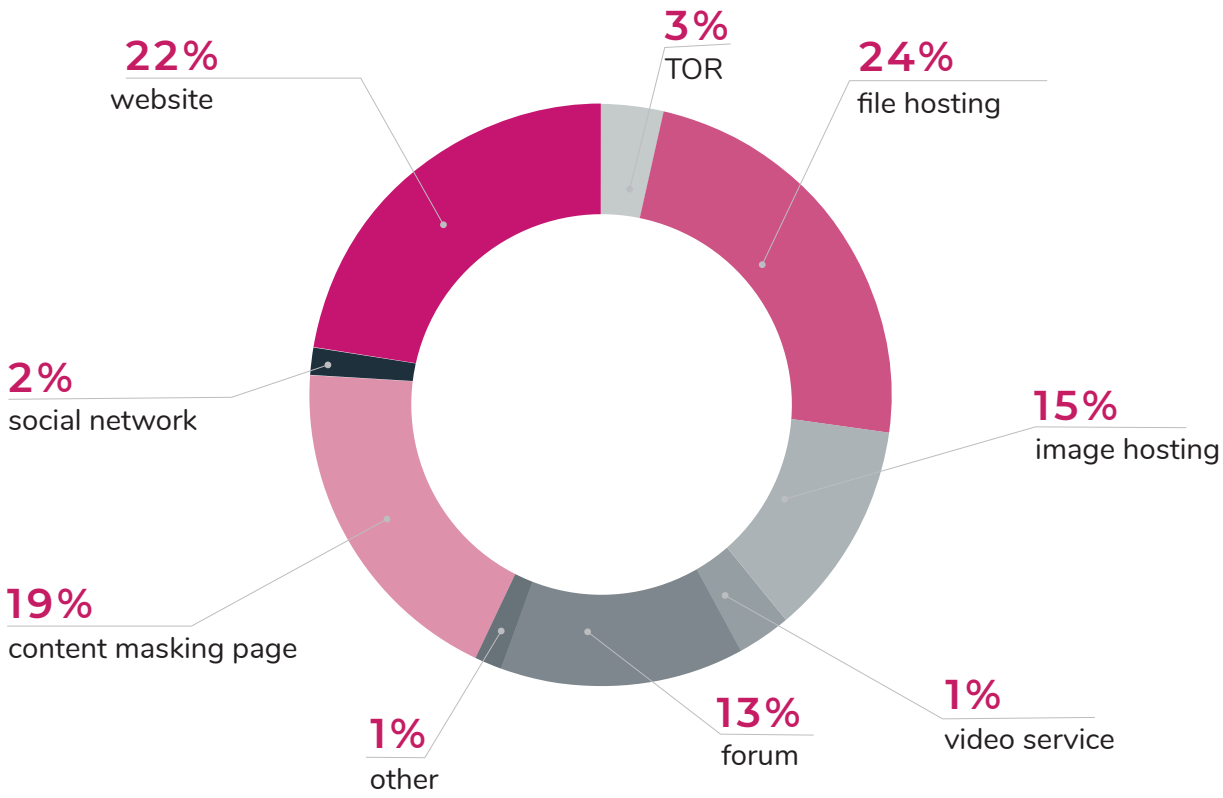
CSAM content analysis

9 Number of reports of potential CSAM-type materials and confirmed CSAM incidents against the total number of incidents analyzed from 2015 to 2021



	2015	2016	2017	2018	2019	2020	2021
Total number of incidents analysed across all categories	14 277	14 298	13 962	13 239	12 517	13 400	14 754
CSAM - applications received in this category	11 227	11 759	11 457	10 784	9 194	8 021	6 778
CSAM - confirmed incidents in this category	3 029	3 126	2 459	1 998	2 295	2 517	2 069

10 | CSAM analysed by Dyżurnet.pl - location in Internet services (n=2069)



Website
A website located on the open resources of the Internet.

File Hosting
A service located on the open resources of the Internet that allows users to upload, view and download files of various types.

Image Hosting
A service located on the open resources of the Internet that allows users to upload, view and download photos and graphics.

Video service
A service located on the open resources of the Internet that allows users to upload and watch video files without downloading them.

Forum
Discussion forums located on open Internet resources on a specific topic; may include multimedia files.

Social network
A service where users create their own profiles and share the content they post with other users.

Content masking page
A Website located in the open resources of the Internet, displaying hidden content after the entry of an appropriate link (http referrer) or cookie.

TOR (The Onion Router)
Resources located in an anonymized TOR network, accessible only through a dedicated browser; most of the above Internet services may have an equivalent in the TOR network. Resource addresses in the TOR network (hidden services) contain the top-level pseudo-domain ".onion".

Out of the total number of 2065 URL addresses on which Dyżurnet.pl experts identified CSAM, 1930 were unique. In other words, repetition accounted for 7 per cent of the total number of CSAM incidents and mainly involved sites masking their content. The specifics of these pages require a corresponding link (URL), which may change over time. Therefore, such sites may be reported multiple times.

11 CSAM analysed by Dyżurnet.pl - number of photo/video files analysed by Dyżurnet.pl and already recognised by INHOPE teams

5 594

Previously recognised by INHOPE teams

3 782

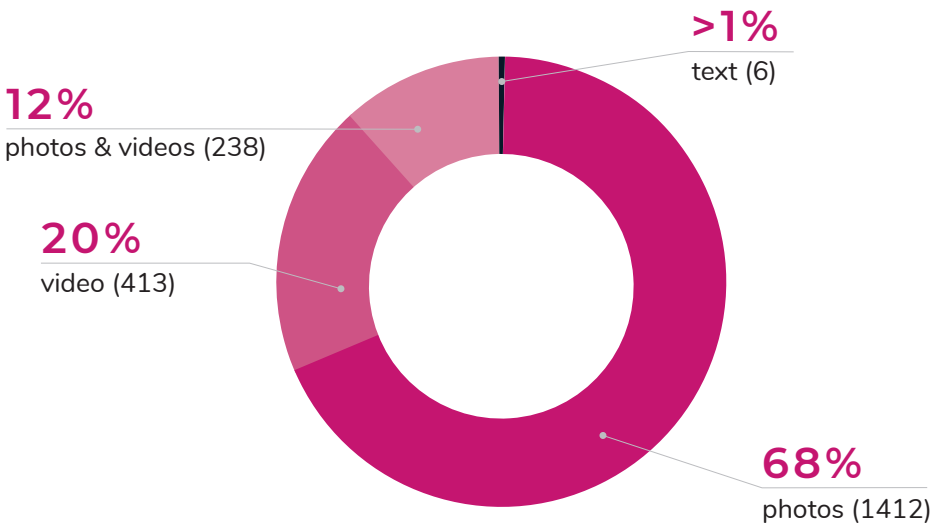
Analysed for the first time by Dyżurnet.pl

The ICCAM database is based on recognizing the hash value (digital imprint) of files. This data is obtained using a hash function to establish short and easily verifiable signatures for arbitrarily large datasets. Analysed and adequately classified images and videos are no longer displayed when re-entering the ICCAM database. This solution avoids duplicating the work of analysts and subjecting them to the stress factors that content analysis entails.

On the other hand, the number of files analyzed for the first time shows the contribution of the Dyżurnet.pl team in building a database of already recognized files containing CSAM.

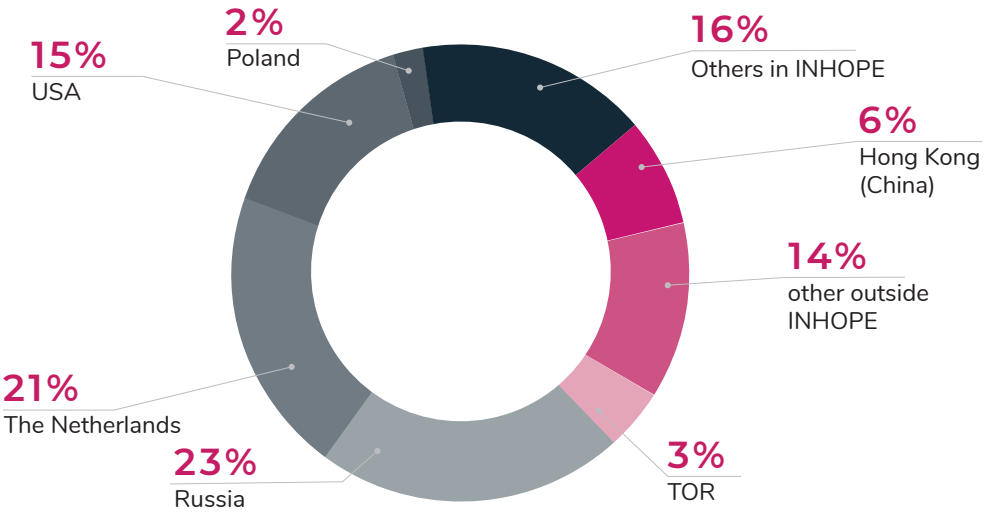
In 2021, the share of content analysed for the first time by Dyżurnet.pl was 40 per cent.

12 | CSAM analysed by Dyżurnet.pl - type of content (n=2069)



61 incidents out of 2069 involved content depicting a generated or processed image of a minor engaged in sexual activity. Such usually computer-generated, and relatively realistic-looking content is not considered illegal in many countries, so it is still present on the Internet.

13 | CSAM analyzed by Dyżurnet.pl - server location in relation to URLs (n=2069)

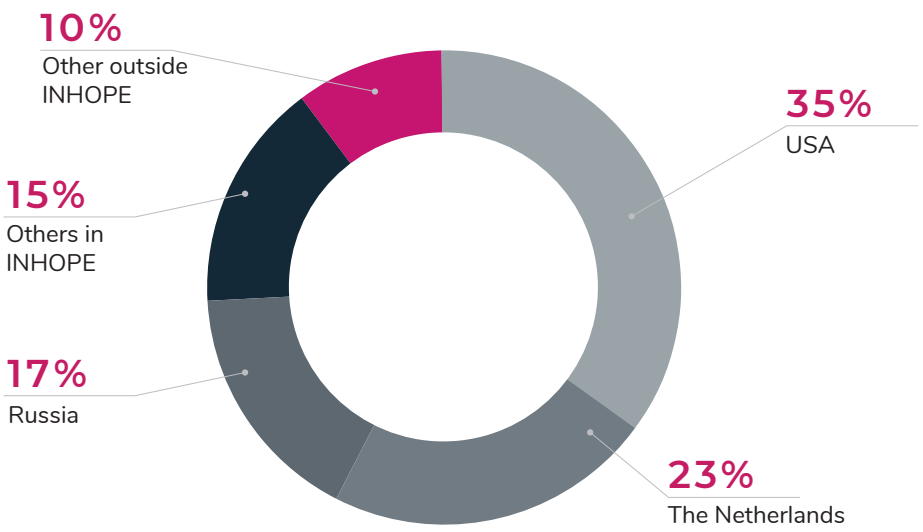


The location of the CSAM content server is critical to an effective response. The Dyżurnet.pl team distinguishes two types of locations:

- with respect to the URL
- for photo/video files

For example - http://abc.com is hosted on a server located in the USA. The location of this type is shown in Figure 13. However, this site's illegal photo or video files are located on servers in other countries, such as the Netherlands or Russia. The location of the CSAM files is shown in Figure 14.

14 | CSAM analyzed by Dyżurnet.pl - location of servers in relation to photo/video files (n-3782)



In 2021, Dyżurnet.pl experts noticed the increasing placement of pages and files with CSAM content outside the scope of activity of response teams affiliated with the INHOPE Association.

In terms of URLs, it was 23 per cent in 2021 (2020 - 7 per cent, 2019 - 11 per cent)

For photo/video files, it was 10 per cent in 2021 (2020 and 2019 - 4 per cent each)

Due to this trend, new standards and procedures have been developed to allow specific Association teams to intervene directly with the foreign hosting provider to remove CSAM content.

15 | CSAM analyzed by Dyżurnet.pl - breakdown by content category (n=3782)

57%

BASELINE CSAM

43%

NATIONAL CSAM

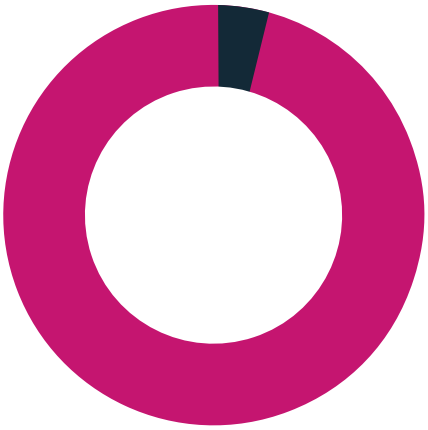
CSAM Baseline (illegality criteria in all countries cooperating with Interpol):

- A picture of a real, live child. Computer-generated images, drawn or otherwise produced or processed, omitted
- Children depicted in sexual abuse situations are prepubescent (have not reached the age of 13)
- Presenting a situation of sexual contact or focusing on the child's genital or anal region

National CSAM

- Pornographic content with minors over the age of 13 (material with younger persons is classified as Baseline CSAM)
- Pornographic content depicting a manufactured or processed image of a minor engaged in sexual activity

16 | CSAM analysed by Dyżurnet.pl - share of self-generated sexual content (n=2069)



92%

NON-SELF-GENERATED CONTENT (1908)

8%

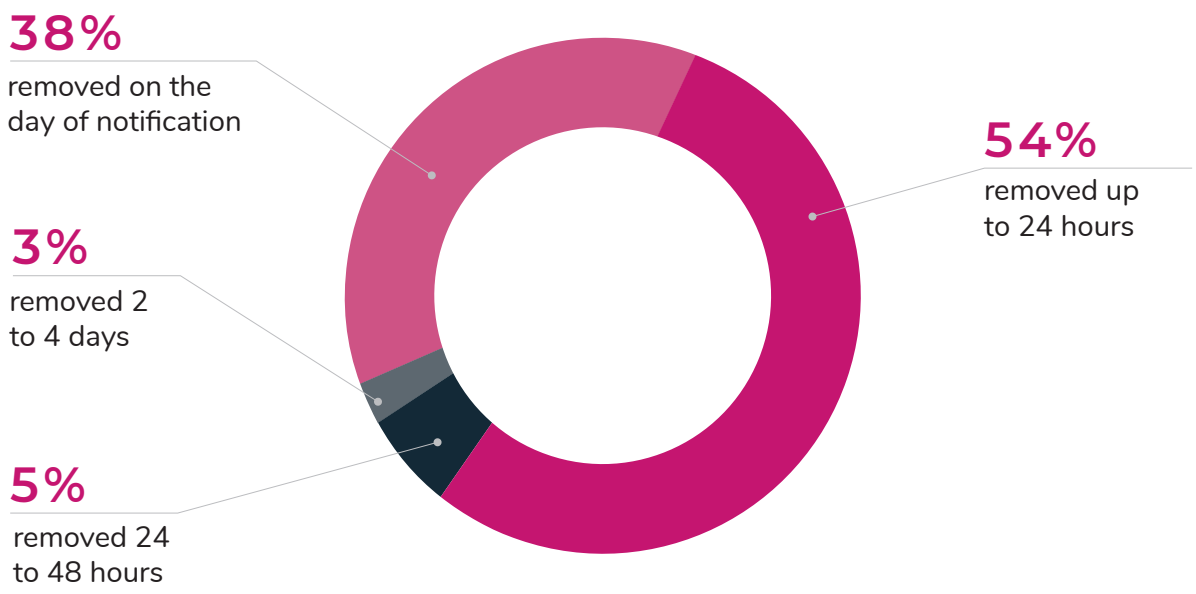
SELF-GENERATED CONTENT (161)

Self-generated sexual content - photo/video material produced independently by a minor, whether obtained with or without the minor's consent, depicting the minor engaged in sexual activity. For more on this topic, see our publication "Risky Sexual Behaviour and the Sexualisation of Young Internet Users. Outline of Issues."[4]

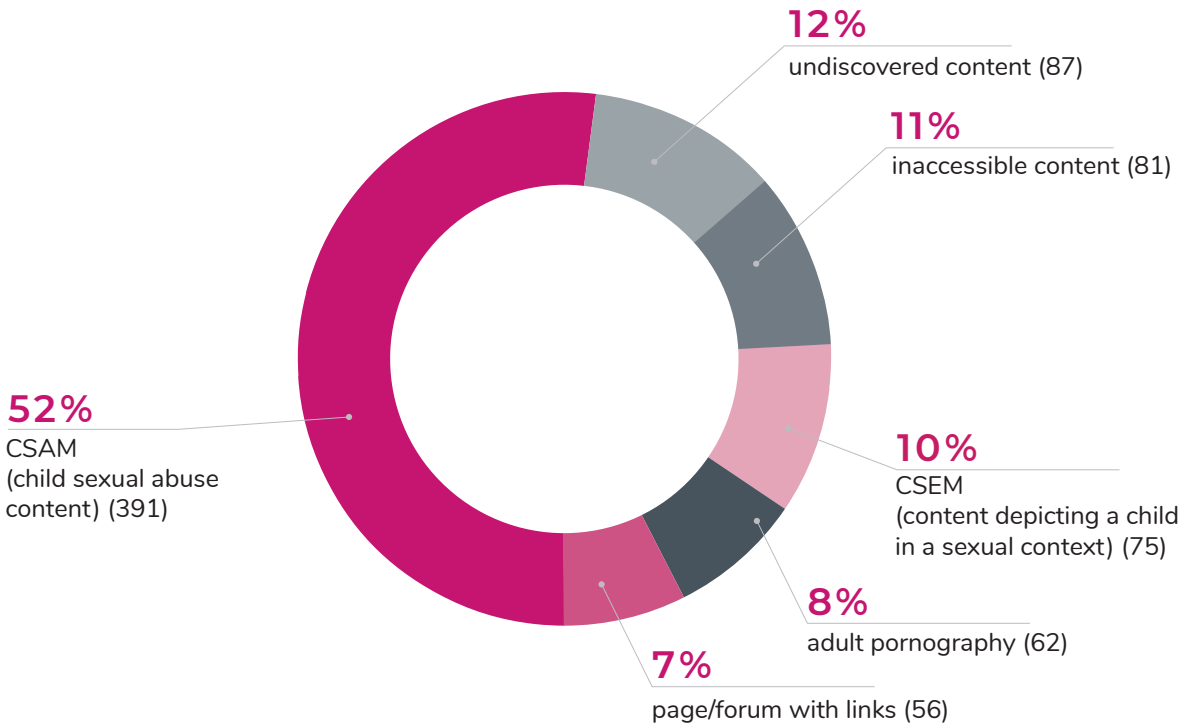
After the increase in the share of this type of material in the total number of CSAM from 9 per cent in 2019 to 14 per cent in 2020, observed by Dyżurnet.pl experts, the number of content classified in this way dropped to 8 per cent. It turned out to be the lowest in 3 years. It is worth noting, however, that isolated incidents usually involve forums where thousands of such materials are posted, produced by both teenagers and early elementary school-aged children. In this regard, experts observe an increasingly earlier "initiation" in the creation of sexual content by children.

4. https://dyzurnet.pl/uploads/2020/04/Ryzykowne_zachowania_na_www.pdf

17 | Time of public availability of CSAM/CSEM located in Poland and reported to Dyżurnet.pl by other INHOPE teams (n=37)



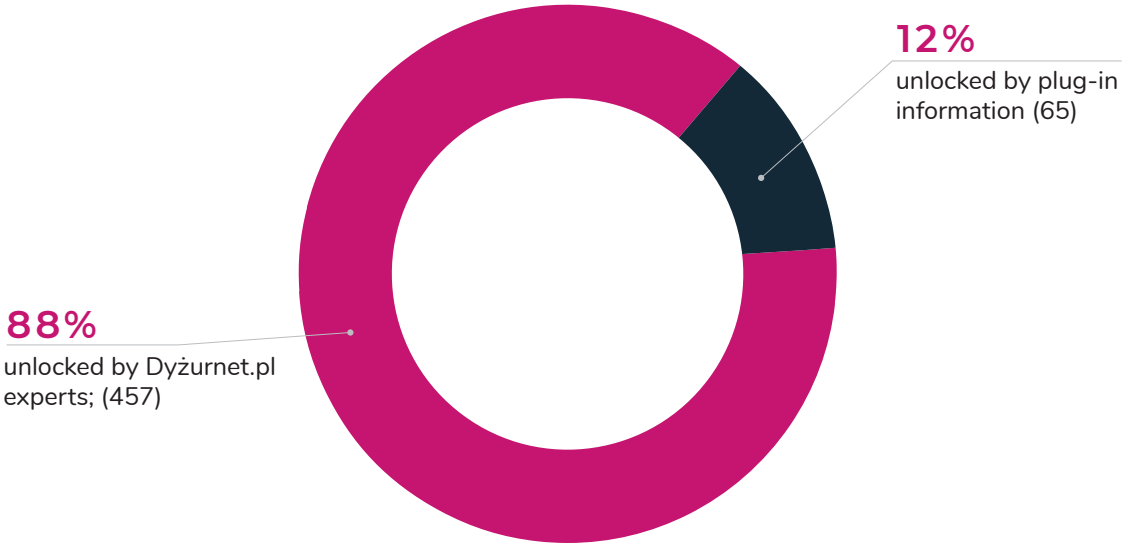
18 | Classification of sites masking their content (n=752)



The number of pages masking their content analyzed by the Dyżurnet.pl team in 2021 was 752, which is comparable to the previous year (in 2020 - 784). Dyżurnet.pl experts managed to unlock hidden content in 70 per cent of cases, which is a much better result than last year when hidden content was unlocked in 53 per cent (a page that displayed content from the following categories is considered unblocked): CSAM, CSEM, links page/forum).

The increased number of reports submitted through the reporting plug-in, which was developed specifically for reporting sites masking their content, has, to some extent, contributed to the improved performance. In 2020, the Dyżurnet.pl team received 91 notifications through the plugin, and in 2021, already 238. The number of sites unlocked due to the information provided by the plugin was 65, representing 12 per cent of the total number of unblocked sites masking their content.

19 | The share of sites masking their content unblocked by information provided through the reporting plug-in (n=522)



Actions taken by Dyżurnet.pl against illegal and harmful content

Since 2015, INHOPE-affiliated response teams have used an integrated CSAM information exchange database. The ICCAM database allows you to classify photo and video files posted at a specific url. Materials are classified based on victim characteristics such as gender and approximate age. It is most important to identify material that constitutes illegal content in all INHOPE member countries (Baseline). Information on the most drastic material is passed directly to the ICSE database (International Child Sexual Exploitation database [6]), enabling action to identify the victims and perpetrators.

In 2021, Dyżurnet.pl experts entered 1 850 reports on URLs containing illegal content into ICCAM. There were a total of 9 376 graphic files and videos classified as child sexual abuse content.

The second most frequent method of intervention undertaken by Dyżurnet.pl experts is direct contact with moderators, administrators, website owners or content authors. This usually applies to legal content that violates community rules or policies. Such interventions are undertaken against Polish and foreign parties and in 2021 took place in 281 incidents.

In 51 cases, the Dyżurnet.pl team contacted hosting providers directly to inform them about their servers' illegal content (concerning CSAM). Public access to the content is blocked, and the relevant data is secured for law enforcement action, who are also notified.

Due to the scope exceeding the scope of operations of Dyżurnet.pl, 107 cases were forwarded to other entities - e.g. CERT Polska team operating within NASK-PIB or intervention phones run by the “Dajemy Dzieciom Siłę” Foundation.

145 incidents were reported to the Police Department's Cybercrime Bureau. They were primarily concerned with child sexual abuse. CSAM-related submissions accounted for 80 per cent of the submitted incidents (on Polish servers - 29 per cent, on Polish-language services - 9 per cent, in the TOR network - 42 per cent). 10 per cent of the submissions involved grooming a child and promoting pedophilic behaviour.
10 per cent of the remaining cases reported to the Police involved other content hosted in Poland (hardcore pornography content, racist content or life-threatening cases).

6. https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

TRENDS AND PHENOMENA

Do you know what your child is uploading to YouTube?

Since spring 2021, the Dyżurnet.pl team has noted an increased number of reports of videos recorded by children of several years old, usually girls. According to those reporting, they may have been exposed to unsafe contact by those sexually interested in children.

For the most part, these recordings were "snippets" or "diaries" of the child's life, such as showing her room ("*room tour*"), dancing or vocal playback to favourite music, presentation of a new bed, new hairstyle, clothes, "playing a game," or general comments. These materials are usually recorded alone in the child's room. However, there are also times when they are recorded together with other minors. They are relatively poor quality due to being recorded with a smartphone or tablet.

Viewership of such videos varies from a few to a couple hundred within the first few days of publication; one video had as many as a quarter of a million views. There is a common theme in these materials - a statement showcasing the thinking of some of the authors of such materials: "*We don't know what to do, but it's our life. And so we have to (...) record ourselves because our lives depend on it.*
If we don't record ourselves, there will be no money (...) We say it live. YouTube is the best in the world!"

Many children present a reflection of the behaviour of their vlog idols in their recorded material. There are statements like "*welcome to my channel*", requests for "*thumbs up*" and "*subscribe*".

It is also worth quoting one of the statements of the approximately nine-year-old author of the material: "*If you have TikTok, then drop by the account, I already have 2K. Just please don't ban me, or I'll hang myself. I've spent 2 years to get to this 2K. If you ban me, I promise you that I will kill myself then.*"

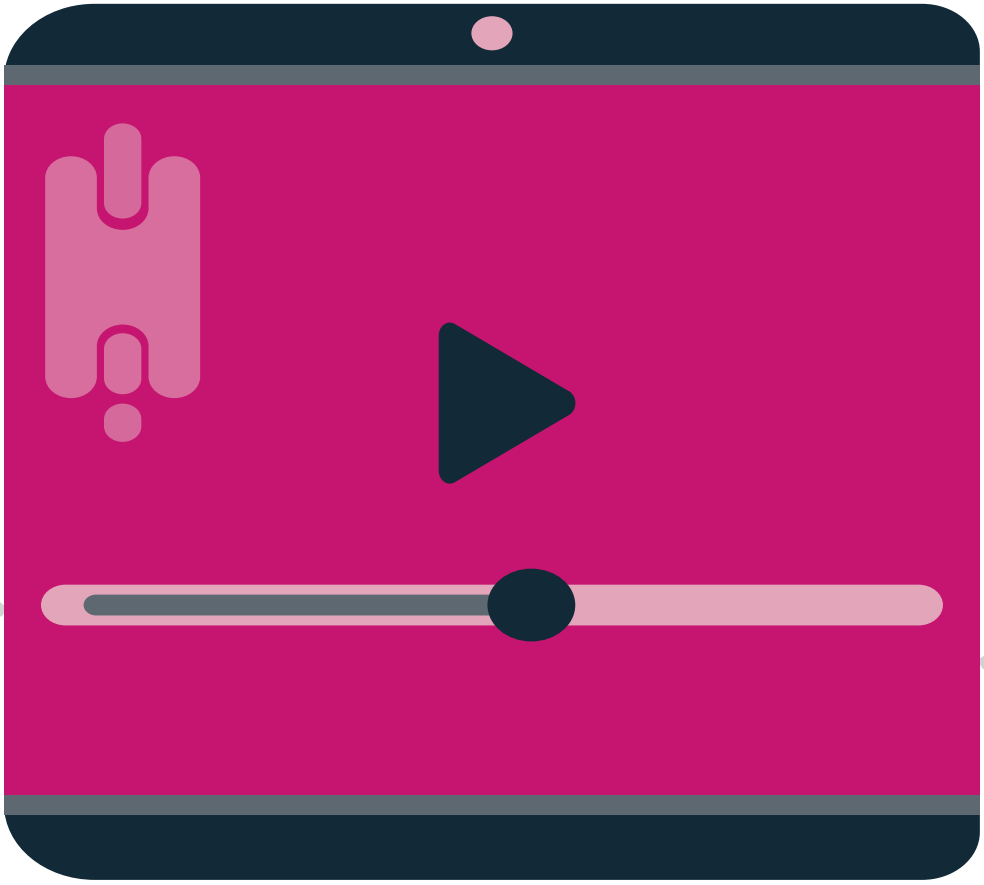
In fact, the actual account of the author had less than a hundred followers. In the material, she referred to the account of another "influencer". Thus, one can see the need to draw attention to oneself or create an intense sensation that the author is willing to post information that misleads the viewer.

Starting in late August 2021, materials of a slightly different type began to appear in large numbers. This time in the form of channels of girls recording and publishing several videos each day. They last a maximum of 15 seconds and present a dance or musical playback. These channels have several thousand subscribers each, and some videos have several thousand views. There are dance routines where girls take off their blouses during the dance and show their underwear or expose their buttocks. Reasons for creating this type of material can range from wanting attention to boredom. There is also a possibility that the child in being groomed. Often young people motivated by the desire to gain popularity on well-known sites undertake such activities.

Whenthe recording equipment is placed on the floor, recording "from below," the underwear of standing or dancing girls is visible, which can actually be of interest to those sexually interested in children.

In case of materials of sexual nature, the Dyżurnet.pl team intervenes and reports them to YouTube, which immediately removes them. It is significant that in the vast majority of materials created by children, the ability to post comments is blocked.

It is worth remembering that publishing a child's image on the Internet may involve a risk both on the part of peers, who may subject the child to harsh criticism, and attract the attention of the persons mentioned above with paedophilic tendencies. It is best to accompany, support and control your child on their way to “becoming a famous influencer."



Grooming a child on the Internet

The problem of child grooming has assumed worrying proportions with the advancement of technology, anonymity in the virtual world, and lack of parental awareness and control[6].

While it is possible to see recurring patterns of interaction used by perpetrators in the data received by the Team, it is worth noting that both the manner of conversation and the reactions of minors are not uniform. Perpetrators may be individuals who resort to blackmail, but they may also offer compensation in exchange for “favours." They may impersonate a modelling agency or an authority (e.g. service administration), pretend to be a person close to the victim's age, or be upfront about their actual age. Some of them hide behind fake accounts from the beginning of the conversation, requesting intimate photos and sending their own photos or videos (often clearly using an automatic translation of the message from another language). However, sometimes these persons are known to the child from another service or real life.

Sample conversation content (original spelling):

- you're in serious trouble
- 😬😱😬
- I will now send our conversations, photos and videos to record all of Europe, you can see your face and body naked, I do not recommend blocking NOW 👍

There are also interactions aimed at befriending or simulating a relationship, building closeness and trust - but there are disturbing elements of seeking to keep the relationship secret - “don’t tell anyone," “this will be our secret," "i’m scared because it’s illegal." Despite the apparent amicability, it is common to see a strong emphasis on sexual content in the conversation and a constant recurrence of this topic - and in doing so, violating and pushing the minor's comfort boundary.

Sample conversation content (original spelling):

" - I can text with you
Don’t tell anyone
- I won’t
I'll do what you tell me
Anything but don’t report it
👍
Anything, please
Whatever you want
If you want, I'll show you on camera
I'll do anything, please
Whatever you want, just don’t report it? Please."

6. https://repozytorium.uph.edu.pl/bitstream/handle/11331/2671/Wrobel-Delegacz.W.Grooming_zagrozenie.pdf?sequence=1 – page 12

Some cases may be characterized by rapid changes in mood - the abuser very quickly moves from an affectionate and asking tone to an angry and attacking style, especially when their demands are not met. For the most part, perpetrators are aware of the consequences they face - they are not always willing to give out their factual personal information or facial photos. Still, they are anxious to obtain pictures of the child.

The purpose of the conversation can vary - some perpetrators want remote fantasy gratification through sexting (which does not necessarily include sending pictures), others aim to meet the child, and still, others want to get as many photos or videos as possible.

Children's reactions to these types of interactions also vary widely, often seeming to be a consequence of ignorance or disgust due to being too young or being interested in sexual topics. This is especially true for children who are a little older. Some young people outright reject new acquaintances because they are too intrusive or direct. Sometimes, because of the perpetrator's age, they don't want to continue a conversation with an adult. Some youth are drawn into highly sexualized interaction. Sometimes young people seek intimacy online and are not always aware of the age of the person with whom they are engaging in a relationship. Such people may be lulled into the narrative that exchanging intimate material is necessary and safe (after all, it is only sent for a "friend" who has promised discretion). In some cases, it may feel as if the child is unaware that a conversation that becomes uncomfortable can be ended at any time and that an overly intrusive interlocutor can be blocked.

A common element of manipulation introduced by perpetrators is to make the young person feel a sense of pride or a need to match their peers - this manifests itself in statements such as "I know people your age who are already doing it", "Are you ashamed?", "Are you afraid?" as well as emphasizing their experience in sexual matters, the opportunity to learn something enjoyable and "adult", the pleasure derived from such encounters, and even the potential direct benefits to the young person - material or monetary compensation. Topics related to sexuality are made as shallow as possible by the abuser. Still, he keeps returning to them despite the child's desire to change the subject. There is also often frequent and intrusive checking the other party is there and available to chat.

Sample conversation content (original spelling):

"Who are you with
Who are you going with, sweetie
You're a sweetheart
😍😍😍😍😍😍😍😍😍😍
Why aren't you writing to me, honey
Are you there baby 😍😍😍😍😍😍😍
Why aren't you writing to me, honey
You're mad at me honey."

Another way of manipulating a child to obtain intimate material is to seek to deny responsibility in conversation, to blame the victim - "if you want, I'll send you...", "if you want, you can send me...", "he/she wanted it herself", and to portray sexual desire as a force independent of the person - "only you can help me... I can't stand it anymore". Although the topic of sexuality is often initiated solely by the perpetrator, how he conversation is conducted creates pressure for complicity and aims to blame the victim. Of course, even in cases where a minor initiates sexting, this is in no way a mitigating circumstance or excuse.

Sample conversation content (original spelling):

"- She asked me herself if I would show her
- She wanted it herself."

The images obtained during these conversations may be used to directly satisfy the perpetrator's personal needs. Still, they may also end up in a pool of pictures exchanged between child sex offenders or be used to blackmail the victim at later stages of the relationship into obtaining more images under the threat of sharing the existing collection with the young person's family and friends. Therefore, it is imperative to dispose of one's image carefully, especially one that can be compromising or highly problematic when taken out of context.

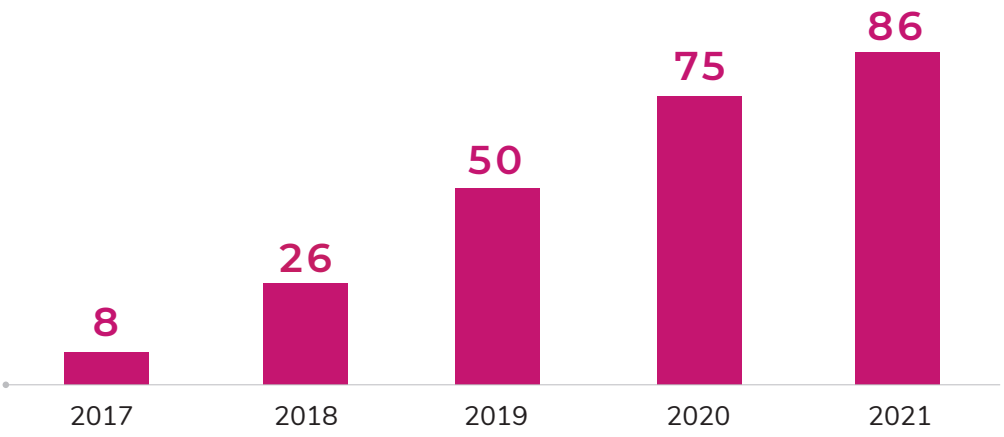
In addition to limiting the trust in people met online (they may not necessarily be who they say they are), it's essential to pay attention to your own feelings and motivations - whether the motivation is your own or due to external pressure exerted in various ways by the other person - by invoking friendship, conditioning the relationship existence, arousing sympathy and a desire to help. Can you easily identify the person in the photo based on the photo you sent? Will it be possible to identify the source of the leak after any "leaked" photos? Perpetrators may want to clearly identify the person in the photo and the "uniqueness" of the photo.

When you share information about yourself on the Internet, you must be aware that it may be duplicated and distributed further. It will be virtually impossible to remove it from the network altogether.

Sexual blackmail

Sexual blackmail is an increasingly common problem noted by Dyżurnet.pl team experts. In the 2020 report, the phenomenon is widely covered and described. This report will focus on the scale of the phenomenon.

In 2021, the team recorded 52 reports of this practice and 34 so-called "sextortion SCAMs," which are reports of automated, mass-mailed messages pretending to be sexual blackmail to extort money. A total of 86 reported incidents were recorded in 2021. As seen in the attached table below, the trend of sexual blackmail reports (also considering "sextortion SCAM") by year is upward. The submissions were primarily related to adults. Only three applications received were for individuals under the age of 15.



Reports of sexual blackmail and sextortion SCAM by year

This statistic shows that adults are very often the victims of sexual blackmail and should have the knowledge and risk assessment skills to guard against this type of threat. Moreover, to a certain extent, it is incumbent upon these people to educate the youngest Internet users, usually their own children, in this regard. Meanwhile, the lack of awareness and interest in digital threats often results in dangerous online activities by adults, so it is worth supplementing the knowledge about this phenomenon. More information on sexual blackmail is available in the publication: ***Risky sexual behaviour and sexualisation of young Internet users***[7]. and in articles by the Dyżurnet.pl team available on the website. They discuss the scale of the problem, point out how easy it is to fall victim to this type of activity without proper awareness, and indicate "best practices" to protect oneself from sexual blackmail.

7. Risky sexual behaviour and the sexualisation of young Internet users. Outline of Issues, Series: Internet - Education - Security, Warsaw, 2019

Content moderation and site regulations vs distribution of CSAM materials

Although Polish law does not regulate the procedures for responding to incidents related to the distribution of CSAM materials, we can observe the positive attitudes of facilitators who join the activities on behalf of abused children. For example, we can mention the moderators of one of the Polish portals who reacted to the incident on their website in an ideal way. In fact, last year, the portal fell victim to an organized plot to provide links on the site that led to child sexual abuse material. Moreover, the users sharing this content were impersonating state institutions and organisations working on internet security. The whole situation has been reported directly to the Dyżurnet.pl Team by the site administration.

However, this is not a standard response, and the European Commission's recommendations even further counter the spread of child sexual abuse materials[8]. Not only is direct cooperation between ISPs and incident response teams recommended, but the need is also stressed to introduce action based on trusted flaggers, including simplified and more effective procedures, allowing for faster removal of illegal content. The introduction of trusted flaggers in service provider systems allows for prioritising requests from trusted institutions, resulting in immediate response.

In addition, according to the WeProtect[9] model, any service that allows users to share their own content should also provide an easy way to report it, a mechanism for responding to incidents, especially those related to child safety. Information about the prohibition of sharing child sexual abuse materials should also be included in terms of service detailing the prohibition of the production, distribution, and display of such materials. Such a portal should also have a unit - a specific staff member or an entire team - responsible for processing requests for CSAM materials. At the same time, however, every employee accepting reports should be prepared for a situation in which they will come into contact with illegal and destructive content, should be informed about the risks, should voluntarily consent to them, and should have the appropriate knowledge and skills to accept and analyze such reports. Each such employee should also be provided with appropriate working conditions, particularly psychological support.

8. Study on Framework of best practices to tackle child sexual abuse material online, 2017
9. www.weprotect.org/frameworks/industry

Children's rights in the digital environment

The vast amounts of user data that are created with digital services require the creation and constant updating of user rights. Due to the need for special protection, children should be provided with the highest standards of safety and application of existing regulations while at the same time giving them space to realize rights such as the right to access the digital environment, the right to free expression and online information, the right to participate and play, the right to learn and media education, the right to protection and safety, and the right to privacy and data protection.

Children use the Internet according to their needs which they fulfil. These needs affect many aspects of their lives on different levels, e.g., the need for interaction, expression, belonging, etc., and as a space for leisure and entertainment. In addition to its many advantages, increasing digitization also brings risks, such as facilitating new types of discrimination such as cyberbullying (online violence) or hate speech spreading online. Above all, young people need to be protected from harmful and illegal online material that they may come across intentionally or accidentally.

Therefore, creating applications or services whose users are or may be children should implement the principle of building these tools based on ensuring the highest possible safety for the youngest users. Many popular sites visited by the youngest users only conduct age verification by asking for birth date, which may not be enough to prevent these tools from being used by people for whom they are not intended based on age. Lack of parental and caregiver verification of applications and services used by the child, resulting from unawareness of risks, can also lead to contact of young users with harmful or illegal materials.

It's worth noting that parents or caregivers often engage in risky or harmful behaviours online that can harm little ones in the future. An important point to note is the issue of privacy, as children also have the right to privacy online, which means that publishing material with your child online should be discussed with them in advance.

Building online safety for children and youth should be based on collaboration among site developers, parents, caregivers, and educators. Knowing the risks and dangers of the Internet and how to protect yourself from them is the foundation of building and creating the Internet.

Can the internet forget?

Often, the Dyżurnet.pl team is notified of content that is not illegal but only illegally shared, e.g. photos made public without the consent of the person captured in them. This type of notification does not fall within the scope of the Team's activities because there is no legal basis for taking specific actions - in such cases, only the victim can do so. This is also valid for publishing sensitive data, such as credit card or bank account information and medical information. In such circumstances, you can take advantage of the right to be forgotten, which every person has under the EU Regulation GDPR, which guarantees every individual the right to request the erasure of their personal data by the controller of that data. Moreover, the data controller is obliged not only to erase the data but also to notify such a request to all other entities to which it has provided the data. However, deletion of personal data is not possible in specific cases. Such a situation may occur, for example, in journalistic activities - if data is deemed of public interest, it may remain undeleted due to the right to freedom of expression and information. Deleting data may also not be possible due to legal considerations, e.g., an employment law provision requires employees' personal data to be retained for a specified period of time, even after the employment relationship ends. Similar rules apply to online retailers and the personal information they process about customers.

The right to be forgotten also applies to results provided by Google and Bing search engines. Here, we can also request that any sensitive data be deleted. According to instructions provided by Google, consideration is also given to whether the data is "inaccurate, inadequate, irrelevant or exaggerated," and the aforementioned public interest is also verified. Any user who notices sensitive or inaccurate data about themselves in Google search results or comes across images published without their consent in image search can report this directly to Google support by filling out the appropriate form. Each case is considered individually, and the reporting person is informed of the decision. However, it is worth remembering that a search engine is only an aggregator of content on the Internet. Removing them from the search results only means de-indexing the pages on which the information appears, meaning that they are no longer visible in the search results of the search engine in question but are still available online. To actually remove the content, you must directly contact the administration of the website where the images were shared, as only administrators can remove material posted on their site.

Although it is formally possible to remove images from Google graphics search results, there are times when difficulties arise. Google may reject a submission due to a faulty URL link or other technical issues. Still, it may also be the case that a given image appears on one or more pages in several or even dozens of copies - in which case removing one of them has no tangible effect; each of these materials would need to be deindexed individually. Suppose the image is associated with an online account created in the past. In that case, it may be easier to delete the said account and thus try to prevent unwanted content from appearing in search results. It may also help to change the settings of such an account. When difficulties arise in enforcing the right to be forgotten, it is a good idea to look for alternatives and perhaps eliminate the material at the source.

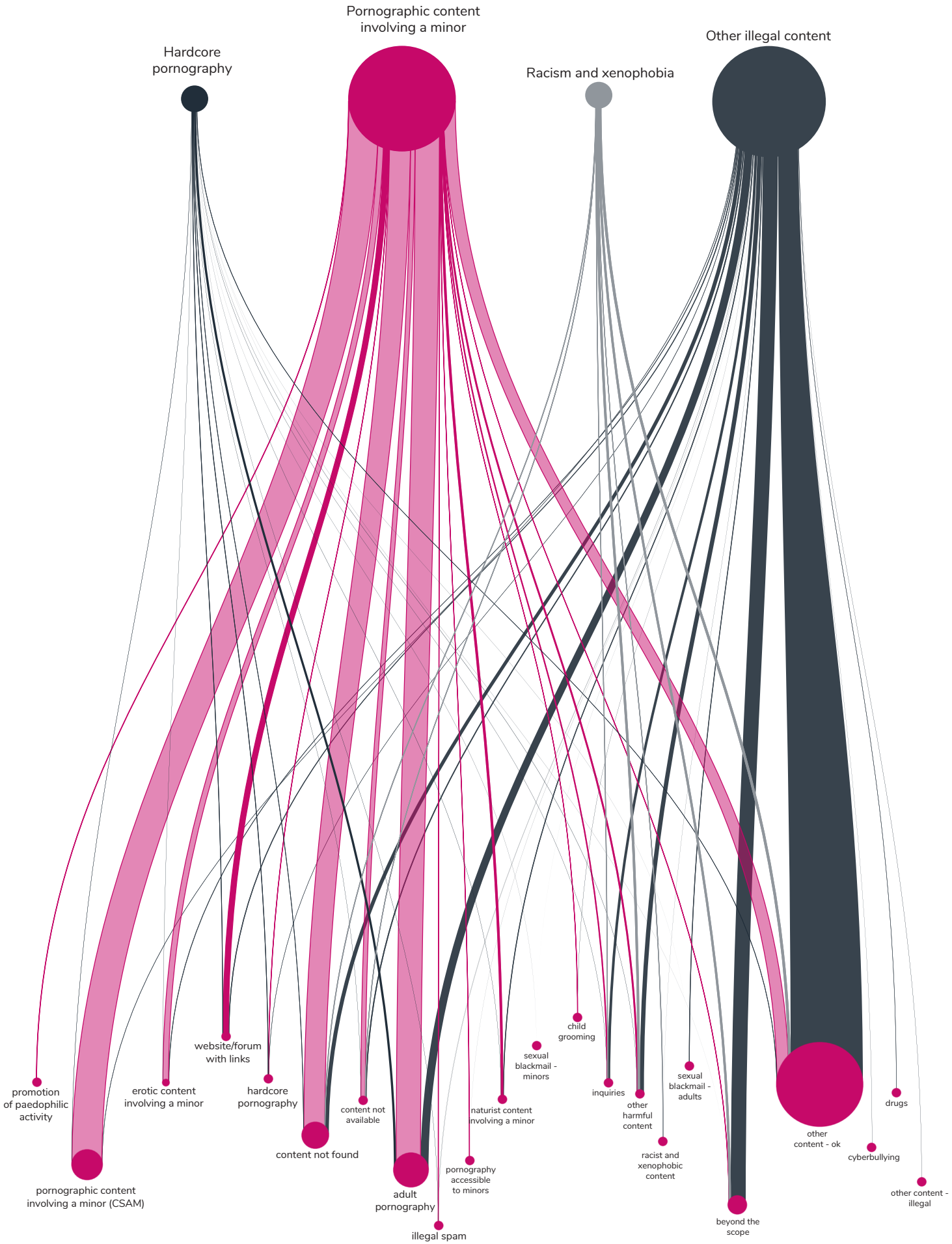
Reporting lawful content

Last year, for the first time, there were fewer reports of child sexual abuse material than incidents in other categories. CSAM photo and video submissions accounted for only 46% of the submitted content. Other submissions often deal with topics related to sexuality - Japanese culture or artistic photo shoots, but nothing to do with child sexual abuse. It is worth noting that, in addition, the form of these submissions often makes it impossible to actually analyse them because the URL link leads to search results, and these can change depending on many different factors.

All notifications received by the Team are analysed individually. Each such case is reflected in the created incidents and thus in their number and distribution of categories (see Dyżurnet.pl Statistics for 2021). This way, search result submissions that include completely harmless and legitimate content significantly impact the team's final performance statistics.

The chart below shows the distribution of useres' reports between categories assigned by Dyżurnet.pl team analysts after analysis. As you can see, the vast majority of the classified material is neutral content (other content - ok), which is reported by users as illegal content, but in reality not only does not break the law in any way but also cannot be considered harmful content. Many reports also concern issues outside the scope of the team's activities, particularly when the law has been broken. Still, the perpetrator is prosecuted only at the victim's request.

Approximately half of all reports are reports of content potentially depicting child sexual abuse. Statistically, in every fifth case, the presence of such materials at the indicated address can be confirmed. Still, often the content is no longer available. Also, very often, the material reported is not CSAM material but adult pornography, so again, legal material.


Pornographic content involving a minor
Hardcore pornography
Racism and xenophobia
Other illegal content
promotion of paedophilic activity
erotic content involving a minor
website/forum with links
hardcore pornography
content not available
content not found
naturist content involving a minor
sexual blackmail - minors
child grooming
inquiries
other harmful content
sexual blackmail - adults
drugs
other content - ok
cyberbullying
other content - illegal
racist and xenophobic content
beyond the scope
pornographic content involving a minor (CSAM)
adult pornography
pornography accessible to minors
illegal spam

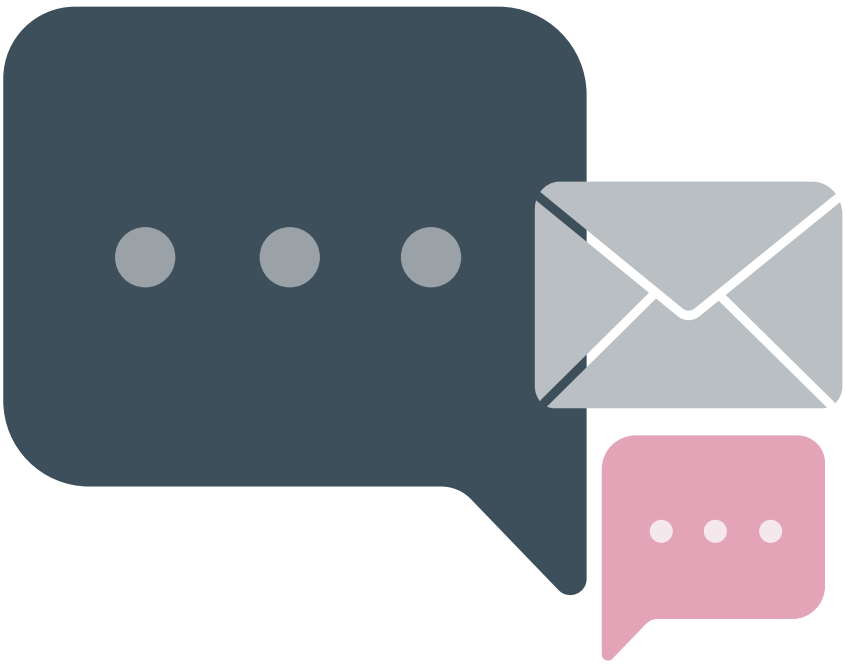
Dangerous online challenges

The Dyżurnet.pl team's reports and publications repeatedly contain information on harmful or, on the contrary, positive messages from Internet challenges. Challenges tend to be promoted primarily on social media, often by people with large followings - celebrities, influencers, and politicians. Such initiatives can spread awareness about a disease or social issue, or simply bring together as many people as possible for entertainment purposes.

Unfortunately, there are also challenges online that may be dangerous - the Tide Pod Challenge, which involves eating a capsule of laundry detergent, sprinkling salt on your body and applying an ice cube to your skin (Salt and Ice Challenge), or the hazardous form of the Ultimate Selfie Challenge, which involved taking a selfie in a daring situation or dangerous location, such as the edge of a cliff.

The Skull Breaker Challenge is one of the newer challenges that have emerged on social media and are gaining traction. It goes as follows: three people standing in a row jump up with the two on the outer sides undercutting the legs of the person in the middle as they jump up. The results of such a “game" usually include bruises, fractures, and in many cases, severe injury or disability.

It is necessary to accompany children and teenagers in their online choices and encourage them not to succumb to fads. Sometimes seemingly innocent fun can lead to disability or death. It is worth making young people aware that being safe online also involves not engaging in or imitating dangerous behaviour in real life.



Harmful content popular among children and youth

Harmful content on the Internet can be encountered in many different ways. For example, such material can be found among the "popular" videos offered by the portal. On social networks, it can be a malicious redirect from another site or a link sent by a friend or even a complete stranger. One form of harmful content is pathostreams. These are live broadcasts of behaviours defined and perceived as pathological, e.g., reports from drunken parties, materials presenting aggressive behaviour or encouraging it towards other persons or specific social groups, name-calling, fights and other dangerous patterns.

Unfortunately, the phenomenon is still present online, and the fight against it is often uneven. Pathostreams constitute harmful material but rarely do they include infringing content. In such cases, removal or special marking of the content (e.g., material not intended for children) is at the site administrator's discretion.

Why are pathostreams dangerous?

- they promote hazardous and harmful behaviours,
- the content contained therein may be illegal,
- they can cause negative emotions in the recipient,
- they urge you to deposit money,
- they paint a hypocritical picture of reality,
- young people encouraged by the popularity of their "idols" may engage in similar activities to gain recognition and fame.

Patthocontent creators, encouraged by donations from viewers, popularity and publicity, decide to undertake increasingly bold behaviour. As the phenomenon grew, the materials included harassment or abuse of others or arson and destruction of objects.

In order to be effective, the fight against “pathostreams" should be based on building awareness about the harmfulness of the phenomenon and its negative impact on young people, as well as on not promoting this type of material on the Internet by the services on which it is posted.

Recently, the media have reported several times on the temporary arrest of known pathostreamers, which shows that taking action to protect young people from exposure to harmful content brings measurable effects.

New technology regulation and security

At the end of December 2020, institutions, organisations, private sector industry representatives and independent experts involved in projects aimed at preventing and combating child sexual exploitation watched with concern as the European Electronic Communications Code (ETC) came into force on 21 December 2020 [10] The consequence of its complete application was that certain online communication services, such as webmail or messaging services, were covered by the e-Privacy Directive[11]. This, in turn, took away their ability to voluntarily detect and report instances of CSAM category materials in their products and services.

Back in September 2020, the European Commission, in an effort to prevent this situation, proposed an interim solution whereby providers of online communication services could continue their voluntary efforts to detect, report and then remove CSAM[12]. The main argument to convince the adoption of this proposal was that it guarantees privacy and personal data protection. Another rationale was that confidentiality of communications should not protect sexual abusers of children. Unfortunately, we had to wait until August 2021 for it to take effect. This is because it took so long for the negotiation process to reach a final agreement on this legislation[13].

Why was intervention by the European Commission necessary?

The private sector's efforts to reduce the presence of CSAM in their products and services are an invaluable contribution to the international community's efforts with a vision of the Internet from this content. The private sector's practices consisting in using technology to automatically detect material previously classified as CSAM[14] by comparing hash data complements the parallel activities of helplines, such as Dyżurnet.pl, affiliated with INHOPE.

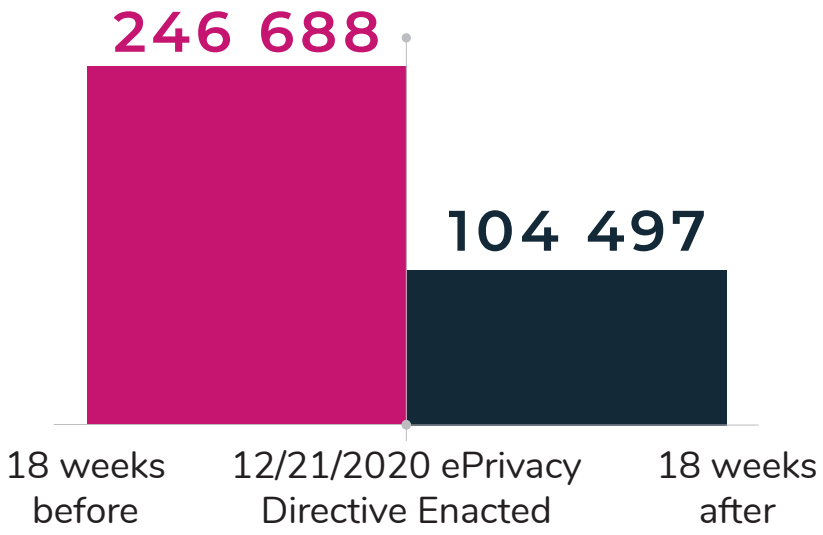
To outline the challenge's scale, it is worth citing data published by the National Center for Missing & Exploited Children in the U.S.[15]. Under U.S. federal law, local private sector entities must report to a hotline managed by the centre - CyberTipline - when material that may depict child sexual abuse is disclosed in their resources. This is a unique regulation with no equivalent anywhere else in the world to date. The figures released by the organisation are alarming: in 2020, CyberTipline received more than 21.7 million reports, an increase of 28% compared to 2019[16].

10. https://eur-lex.europa.eu/eli/dir/2018/1972/2018-12-17
11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219
12. c.europa.eu/home-affairs/news/eu-will-continue-protect-children-sexual-abuse-online-2020-09-10_en
13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2021.274.01.0041.01.ENG
14. c.europa.eu/home-affairs/news/eu-will-continue-protect-children-sexual-abuse-online-2020-09-10_en
15. https://www.missingkids.org/HOME
16. https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers

The situation, as it stands in December 2020, should be clearly defined in the following terms: without the temporary provisions allowing derogation from the articles of the e-Privacy Directive detailed therein, the territory of the European Union could become an unrestricted online distribution centre for CSAM. Not surprisingly, the European Commission's proposal has received overwhelming support from those involved in efforts to prevent and combat child sexual abuse. The INHOPE Association launched the "See no evil, hear no evil" campaign, encouraging people to publicise the situation[17]. Even though the problem concerned the European Union, the American NCMEC, already mentioned here, also joined the efforts. In addition to launching a dedicated campaign[18], representatives of this centre have sent more than 200 letters to members of the European Parliament.

What lessons can be learned from a period when such desirable private sector practices were partially abandoned?

According to data released by NCMEC, there was a significant decrease, as much as 58 per cent, in the number of European Union country reports submitted to CyberTipline, comparing the 18-week period before and after December 21, 2020, as shown in Figure[19] below:



Adopting the European Commission's temporary solution is a temporary respite from the crisis, as it has a limited duration - until August 3, 2024. A new package of legislation is currently being developed to govern this area. They are expected to be announced in the coming months.

17. https://inhope.org/EN/articles/e-privacy-directive-temporary-derogation
18. https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety and change.org/ childsafetyfirst
19. https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

Technological solutions

APAKT - project progress

In 2021, the Dyżurnet.pl team will continue the APAKT project, carried out with NASK scientists and researchers from the Warsaw University of Technology and Enamor International technology company, and financed by the National Centre for Research and Development. The project aims to create tools for analysing and detecting multimedia content and textual material shared in cyberspace depicting child sexual abuse.

The methods developed will be based on content classification models built using artificial intelligence algorithms that will, among other things, classify and prioritize reports of online content for the presence of child sexual abuse material.

A prerequisite for the project's success is collecting a considerable amount of data, which will be used to train models based on neural networks. Data consisting of images, videos and texts must be classified and tagged accordingly. Each element of the analysed material, which affects its classification, will be appropriately described according to the adopted and previously developed tagging system.

Selecting tags for particular content types is a significant part of data collection for teaching artificial intelligence models. Mislabelling or inadequate labelling choices can weigh on the end result, which is the ability of a given model to correctly classify content. The extensive experience of the Dyżurnet.pl Team in analysing and classifying CSAM content allowed for precise identification of specific features in the analysed content. All the characteristics that determine the membership of a given content in a particular class of materials were identified.

The next step was to develop tag lists in each group of materials (images, video, text) to train artificial intelligence models based on neural networks. At this stage, the Dyżurnet.pl team cooperated closely with scientific teams from NASK and the Warsaw University of Technology.

ENAMOR INTERNATIONAL Sp. z o.o. has prepared the first version of an IT system that will make it possible to collect data that will be classified, tagged with a pre-selected set of appropriate tags and, in this version, will be continuously transferred to the learning process of AI models.

Plugin for reporting illegal and harmful content

Illegal or harmful Internet content can be encountered by accident by clicking on a link or advertisement that someone has sent. Sometimes websites redirect to content that users would not knowingly choose to view.

To make the content reporting process easier and more efficient for the user, the Dyżurnet.pl team created a special plug-in that, once installed, makes it possible to report illegal or harmful content in just a few clicks. The submission procedure using the Plugin does not require transferring the address of the submitted website to the submission form. It also does not require additional steps other than a simple click on the Plugins icon. Additionally, as with the form, submissions can be made anonymously, and complete data security is guaranteed.

- Mozilla Firefox browser plugin: Report content to Dyżurnet.pl[20]
- Google Chrome browser plug-in: Report illegal content to Dyżurnet.pl[21]

Cooperation with OSE

NASK - The National Research Institute is the operator of the OSE network (ose.gov.pl). The Nationwide Educational Network allows schools across Poland to connect to fast, free and safe Internet. The Ministry of Digitization created the project in cooperation with the Ministry of Education

Dyżurnet.pl experts perform tasks related to increasing online safety, including supporting the definition of safety policy, accepting reports on incidents related to illegal content and co-creating educational and promotional materials.

SYWENTO application

In their work, Dyżurnet.pl analysts collect large amounts of data, which could be used to facilitate the work of other professionals dealing with materials presenting sexual abuse of minors. To this end, the SYWENTO application, a tool created by NASK PIB for computer forensics experts, was created in 2020. It assists in analysing Internet address (URL) data for the presence of pornographic content involving minors. After sending a query containing a list of Internet addresses visited by a suspect, SYWENTO delivers feedback with a list of URLs previously identified by Dyżurnet.pl team as sites containing pornographic content with the participation of minors and with a date when a given site was analysed by Dyżurnet.pl. SYWENTO system database includes only URLs that have been submitted and analysed, and classified by Dyżurnet.pl. Such information can be helpful when large amounts of material extracted from the media of paedophilia suspects need to be analysed. The result of the query answers if and how often the suspect browsed websites where there was illegal content, according to Dyżurnet.pl analysts.

20. https://addons.mozilla.org/pl/firefox/addon/zglos-tresc-do-dyzurnet-pl/
21. https://chrome.google.com/webstore/detail/report-illegal-content-to/djegpdbohfkhkiebfdikclmmbpgdblbh

ACTIVITIES
education and awareness-building

Campaign

In this day and age, social media is the space where young people create and build relationships, form their own identities, express themselves, and learn about the world around them. With the rise of digitisation, it is a natural consequence that intimate relationship building has also moved to the online world. Year after year, the number of erotic materials produced by young people is increasing, and the phenomenon's growing trend is noticeable worldwide. According to a study conducted by THORN[22] in the United States:

- 2 in 10 girls (ages 13-17) have shared intimate material;
- 1 in 10 boys (ages 13-17) have shared intimate material;
- 40% of the children surveyed agreed with the statement "it's normal for people my age to share intimate material with others."

Many teenagers confirmed positive feelings about their experiences of sharing intimate materials, such as increased confidence or increased feelings of trust. Intimate relationships and flirting online are becoming normalised. Still, at the same time, a growing number of those want to take advantage of this situation. Sharing intimate materials online exposes children to abuse from adults who may seek to use them for various purposes and harassment from peers who may pass the material on to outsiders or make it public. According to NASK's 2021 "Nastolatki 3.0" [23] survey, receiving intimate materials was confirmed by 8.3% of respondents. Young people are often unaware that material can be made public without their consent and that the person they meet online is not always well-meaning or who they say they are. The most prominent threat is the loss of control over what happens to the material once it is posted or made public. Young people are at risk of violence from peers or adults, and materials can also get into the hands of people with pedophilic tendencies. Young people are just as often victims of receiving unsolicited intimate material from others, sometimes strangers, through messages on social media or gaming platforms.

22. https://www.thorn.org/self-generated-child-sexual-abuse-material-attitudes-and-experiences/
23. https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html

In response to the growing problem, NASK has prepared a campaign that addresses the popularity of sharing intimate material among young people and will mainly target teenagers (aged 13-17). Through the campaign activities, the dangers of such activities and places where individuals can turn to for help were indicated, as well as how to proceed in a situation when the materials are made public by persons who gained access to them.

Educating young people to develop an awareness of choice is an important aspect of the campaign - if they do not want to share intimate material, they can always say "no" - the survey showed that an assertive attitude and refusal are not always taken into account by young people, it often stems from a sense of obligation.

The campaign was implemented by the NASK National Research Institute as part of the activities of the Polish Safer Internet Program Center (PCPSI).

PUBLICATIONS

PREPARED

BY: DYŻURNET.PL

The Digital Footprint of a Young Child

In July 2021, the Dyżurnet.pl team released a publication titled „The Digital Footprint of a Young Child[24]". This is a valuable report created by the Team's experts based on their observations of content reported by Internet users. The Team's experts have daily contact with collections of pedophilic material in their work. In addition to content that violates Polish law, they have to deal with legal and seemingly neutral material featuring children. These are photos and videos collected mainly from various social media sites. Most of them have been posted online by wayward parents who are unaware of how the material can be used later.

The report shows the extent to which photos and videos featuring children are published by parents. This is best illustrated by the following quote:

"Among the 168 Polish social media accounts surveyed in 2015, almost 40% posted more than 100 photos of their child, and as many as 90% included the child's name and nearly 84% the child's date of birth. The more information, the more complete an image can be built, ultimately leading to identity theft. A 2019 study shows that 40% of Poles regularly post photos of their kids on various social media sites. Interestingly, 81% of parents rate sharing photos of their own children positively or neutrally. As many as 57% of respondents say that a child's privacy is up to the parents, and there is nothing wrong with uploading photos or videos of the child on the Internet. It is also disturbing that as many as 60% of respondents share documentation of their children growing up at least once a month. Only approximately 25% have asked their child's permission to share their photos" (p. 7).

Key findings from the publication "The Digital Footprint of the Young Child":

- The publication reveals the dangers of carelessly publishing images of children.
- It presents a set of best practices to help parents of young children skillfully manage their children's image.
- It emphasizes the importance of the child's privacy.
- In addition, the report is also aimed at child care facilities. It outlines the most critical aspects of child image privacy that facilities should pay special attention to.

24. https://dyzurnet.pl/uploads/2021/07/Cyfrowy_slad_malego_dziecka.pdf

MOBILE APPLICATIONS

are our children safe?

Every year there is increasing virtualization of the surrounding reality. Mobile apps serve many people in their daily lives every step of the way. In addition, the popularity of touchscreen devices makes apps increasingly easy to use. In many of them, the interfaces facilitate intuitive navigation even by the youngest users.

Apps serve multiple purposes - they entertain, educate, and connect. Using these apps and their functionality allows the needs of young users to be met on different levels - such as the need to belong, the need to connect with others, or the need for expression. For this reason, children are often drawn to products designed for older age groups. Sometimes children, encouraged by their popularity, reach for apps designed for older users, inflating their age for product installation, which can lead to exposure to content intended for older users. Unfortunately, low awareness among caregivers on how to properly configure devices and profiles to limit contact with inappropriate content influences children and teens to use apps designed for older age groups on basic settings - not protecting younger users from content that is inappropriate for them or contact with a stranger.

Using inappropriate apps can expose the youngest user to dangers such as:

- exposure to inappropriate - harmful and illegal - content;
- contact with dangerous people;
- disclosure and leakage of private information;
- perpetuating unsafe behaviours and habits;
- fraud;
- viruses and hacking attacks.

Choosing an app a child can use is not an easy task for the caregivers. The attractive interface, popularity of use among other children, the lack of time to learn about the app, and the low digital competence of parents mean that the installation and quality of the content available in the app do not undergo the scrutiny of caregivers. It's also common for younger children, and certainly teenagers - the child installs them themselves without the parent's knowledge or consent.
The report identifies recommendations for caregivers and parents as well as general potential risks and safety rules for using mobile apps by children and teens. We encourage you to read the Report on Dyżurnet.pl.

Events

In 2021, Dyżurnet.pl representatives shared their experience and knowledge at events, among others:

09.02.2021

DBI - Self-directed, not voluntary - Internet content created by young people

17.03.2021

Sexting and nude photos online - safe in the network with OSE

13.04.2021

Independent doesn't mean voluntary for “Przystań w Sieci”

18.05.2021

DBI - Safer Internet Local Conference

23.11.2021

Self-generated sexual content - Safer Internet local conference

In addition, the expert team co-hosted webinars with the Virtual Chair of Ethics and Law:

- The phenomenon of child sexual abuse in cyberspace and the public-private response to its challenges.
- Implementation status analysis of Directive 2011/93/EU.
- Analysis of the consequences of the entry into force of the provisions of the European Electronic Communications Code.
- Analysis of the implications of announcing a set of rules for all digital services operating in the European Union, the Digital Services Act.
- Analysis of the new legislation package announced by the European Commission to implement the EU strategy to fight child sexual abuse more effectively (if notified before the webinar date).

ABOUT NASK

NASK is a state research institute supervised by the Chancellery of the Prime Minister.

The key field of NASK's activity is activities related to ensuring Internet security. Responding to incidents compromising network security in Poland and coordinating activities in this area is handled by the Cyber Security Centre Division, including the CERT Polska team (www.cert.pl). According to the Act on the National Cyber Security System, NASK-PIB has been designated as one of the Computer Emergency Response Teams, the so-called CSIRT, which coordinates the handling of incidents reported by operators of critical services, digital service providers, and local government. All users can also report incidents to the NASK CSIRT. NASK contributes to analytical, and research and development facilities for the national cybersecurity system.

NASK also conducts research and development activities in developing solutions that increase ICT networks' effectiveness, reliability and security and other complex network systems. Our approach to creating solutions for current and future clients' needs sets our research institute apart from strictly commercial enterprises. At NASK, researchers view commercial problems in the framework of science, using its tools, often broader and more abstract, to arrive at results that are not only satisfactory but also innovative. The mainstream research consists of cyber security understood as detection, warning, incident response, data acquisition, analysis, processing and transfer, and complex network systems, including IoT systems and mobile ad hoc networks. Research on biometric methods of identity verification in service security has an important place in the program. As a telecommunications operator, NASK offers innovative ICT solutions for financial, business, government and academic clients. NASK also maintains the name registry in the .pl domain (www.dns.pl).

NASK

Glossary

CSAM
child sexual abuse materials - materials depicting the sexual abuse of a child. Categorized by Dyżurnet.pl experts as pornographic content with participation of minors (art. 202 of the Penal Code).

CSEM
child sexual exploitation material - materials presenting a child in a sexual context, which are abusive towards the child. However, in most countries, including Poland, these materials are legal.

Report
a submission regarding potentially illegal Internet content sent by a user or institution.

Incident
your submission will be analysed and appropriately classified by Dyżurnet.pl experts.

ICCAM
a CSAM information exchange database available to INHOPE-affiliated teams, to which material classified as depicting child sexual abuse is submitted on an ongoing basis.

ICSE
International Child Sexual Exploitation database - a database maintained by Interpol to which information on the most drastic material in the CSAM category is submitted so that action can be taken to identify both victims and perpetrators.

INHOPE
a network of trusted response teams dedicated to eliminating child sexual abuse material and supporting national procedures to remove illegal material as quickly as possible. The activities of the Association are supported by Interpol, Europol, Virtual Task Force, European Financial Coalition, INSAFE, ECPAT and global IT companies.

Sexual blackmail
(formerly sextortion) is when a perpetrator obtains sexually explicit material and then extorts money from her in exchange for not sharing the material online. Sometimes the perpetrator may demand more videos, photos, or other compensation.

dyżurnet.pl

NASK