renew europe.

# Background for 2 June 2023 conference Protecting Children Online: Between Safety and Privacy

**Shortly**

The volume of CSAM – child sexual abuse material – is rising.

- Increase of reports of 35 percent in 2021 compared to 2020
- Of 29.3 million reports, 29.1 million were from websites and online services
- 62 percent of all known CSAM in 2021 was traced back to an EU country
- In 2021, 82 percent of CSAM depicted children under 13
- In 2021, we see a new trend in images that are made by the children themselves
- But getting the real numbers is very difficult, we simply do not know what is out there in real terms

Current situation

- Interim Regulation currently in place
- It allows for the processing of personal data and communications to fight CSAM
- It gives the possibilities for social media and chat services to detect, report and remove CSAM on a voluntary basis
- The derogation is only valid until 3 August 2024

New proposal

- The Commission made the proposal on 11th of May 2022
- It requires for example websites, social media and chat services to proactively search for CSAM and grooming activities
- Grooming for example is approaching children to convince them to make sexual images of themselves and share it online

Details of proposal

- Websites and chat services need to assess whether their services are at risk of being used for spreading CSAM
- They need to consider having age verification in order to limit children from using high risk services
- National authorities would evaluate the risk assessments and can decide request a so-called detection order, when the social media or chat service is too high risk
- The detection put an obligation then on the website or chat service to deploy automated scanning for CSAM or grooming

Controversy

- EU law and case law of the EU Court of Justice prohibit general data collection and general monitoring – scanning and controlling.

- But with a view to fight the spread of CSAM, the Commission argues it is proportionate to allow national authorities to impose detection orders

Concerns from other organisations

- The European Data Protection Board and Data Protection Supervisor were critical, and raised concerns about whether the Regulation would be effective, measures are too drastic and the consequences to end-to-end encryption
- The legal service of the European Parliament and the legal service of the Council raised similar concerns

**Thorough explanation**

Volume of CSAM is rising, reporting of suspected online child abuse increased by 35 percent in 2021 compared to 2020. Of the 29.3 million total reports, 29.1 million were from electronic service providers (ESPs), as defined by the US-based non-profit organisation National Center for Missing & Exploited Children (NCMEC). According to the UK-based Internet Watch Foundation (IWF), 62 % of all known CSAM in 2021 was traced to an EU country.

According to the international hotline organisation INHOPE, in 2021 82 % of CSAM depicted children aged under 13. The materials include not only already known CSAM materials that have circulated for years on the internet and that have already been identified or hashed, but also new self-generated images and videos. In fact INHOPE identified self-generated content as the trend of 2021. A recent Europol-assisted operation in Germany exposed an offender ring with 400 000 members – the 'Boystown' dark web forum, showing the large scale of these hidden paedophile networks. For instance, the UK's National Crime Agency estimates the number of people who pose a sexual threat to children at between 550 000 and 850 000.

Quantifying the precise volume of CSAM is difficult, as there are numerous ways in which it can be disseminated online, and knowledge about its existence – a fraction of what is really out there – is obtained from reports provided by the ESPs and by non-governmental organisations (NGOs), users and hotlines, on a voluntary basis. The global community relies on voluntary initiatives undertaken by ESPs to detect, report, and remove child CSAM on their platforms. In the US, once companies have removed such content, they report it to the NCMEC, as required by US federal law. The NCMEC then makes these reports available, voluntarily, to law enforcement agencies worldwide.

When it comes to existing EU legislation to combat online CSAM, Regulation (EU) 2021/1232 (the Interim Regulation) currently prevails in the EU. This Interim Regulation provides for a temporary derogation from certain obligations under Directive 2002/58/EC (the e-Privacy Directive), which protects the confidentiality of communications and traffic data. The temporary derogation has enabled providers of number-independent interpersonal communications services to continue voluntary practices of detecting, reporting and removing child sexual abuse material online since Directive (EU) 2018/1972 (European Electronic Communications Code) entered into force at the end of 2020. This derogation will apply until 3 August 2024, or until an earlier date if the current proposal for a regulation is adopted by the legislators and repeals this temporary measure.

**Details of proposal**

On 11th May 2022, the Commission proposed a proposal that would require interpersonal communication services and others to proactively search for CSAM materials and grooming activities targeting children.

The proposal contains mandatory EU rules to prevent and combat child sexual abuse online, covering both old and new CSAM as well as grooming of a child user, notably by imposing detection, reporting and removal obligations on certain online service providers including mainly hosting service providers and providers of interpersonal communication services (i.e. 'providers'). Rules apply irrespective of the provider's place of establishment so long as it offers services in the European Union. The three specific objectives of the legislation are to:
1. ensure the effective detection, reporting and removal of online child sexual abuse (CSA): this includes the dissemination of known or new CSAM or grooming of a child;
2. improve legal certainty, transparency and accountability and ensure protection of fundamental rights;
3. reduce the proliferation and effects of child sexual abuse through harmonisation of rules and increased coordination of efforts.

In order to improve coordination, the proposal aims to establish an EU centre on child sexual abuse (EUCSA), as a decentralised agency to enable the implementation of the new regulation.

- Risk assessment and mitigation

Providers would be required to assess and mitigate risks for each of their services ('risk mitigation'). Moreover, providers, including app stores (or apps) would have to consider age verification and age assessment methods to limit the risk of children downloading apps which may expose them to a high risk of grooming.

- National coordinating authorities

There will be a national CA designated by each Member State that will be in charge among other things of receiving the risks assessments and mitigating measures. They will also play a role in ensuring the effective detection, reporting and removal of online CSA.

- Detection orders

The proposed legislation includes a detection order procedure.15 If the CAs are of the opinion that there is evidence of a significant risk of misuse of a service after looking into the risk assessment and risk mitigation analysis provided, they must consider asking for a CSA detection order on the specific risks identified by the provider. This would happen after considering that the reasons for issuing the detection order outweigh the negative consequences for the rights and legitimate interests of all parties affected. Before any detection order is issued, the service provider must be consulted. If the CA considers that the risks remain significant despite the mitigation measures, it would have the power to request a judicial or administrative authority to issue detection orders by using indicators provided by the EUCSA that will be created. These would require the provider to deploy automated content recognition technologies to detect CSAM or grooming. The legislation leaves the choice of the technologies to the operator concerned, provided that the technologies meet the safeguarding requirements of the regulation. The proposal requires that the providers deploy technologies that are the least privacy-intrusive. Where potential detection would involve high-risk processing, or in every case relating to the detection of grooming, the provider must conduct a data protection impact assessment and consult the data protection authorities.

Detection orders would have to be targeted and specific to what is strictly necessary. In particular, detection must be for the time needed (maximum 2 years for CSAM and 1 year for grooming) and apply to the relevant part of the service, where identifiable.

The EUCSA would forward reports to the competent law enforcement authority or authorities of the Member State likely to have jurisdiction and to Europol. It would also verify if the provider has removed the material, or otherwise refer the matter to the relevant national CA. If necessary, the national CA would request the court or administrative authority to issue a removal order. The CA would also have to request the competent judicial or independent administrative authority to issue an order obliging a provider of internet access services to block access to specific CSAM items that could not reasonably be removed at source. The proposal sets binding conditions for the order to be requested or issued.

Providers should report the required information for competent law enforcement authorities to be able to assess whether to initiate an investigation.

As removal or disabling of access may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress. However, there can be exceptions to this to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

EU law and CJEU case law prohibit the prescription of general data retention obligations and general monitoring obligations. Nevertheless, with a view to combating CSAM and protecting children's rights, the Commission is proposing to allow competent judicial or independent administrative authorities to impose orders on certain providers to scan communications or block websites.

- Judicial redress

The proposal provides for judicial redress, with both providers and users having a right to challenge any measure affecting them. Users have a right of compensation for any damage that might result.

- Role of providers and reporting obligations

Depending on the CSA material under scrutiny (known CSAM, new CSAM or grooming), the providers concerned will have to deploy different technologies with varying levels of human oversight to detect such material. When it comes to known CSAM, technologies used for its detection are typically based on hashing, which can be described as a digital fingerprint. The hash extracted from a potential CSAM is compared to an existing database of hashes. As these technologies already have a very high accuracy rate, providers do not need to perform any human oversight since the verification of the illegality of the CSAM will be done by the relevant authorities.
In contrast, considering the relatively high rate of false positive for unknown CSAM and grooming, under the proposal the detection of such material will requires an additional degree of human oversight. This opens up the question of how such human oversight is supposed to be organised on the side of providers. For the detection of grooming, text-based pattern detection is deployed. For one of these tools, Microsoft reports an accuracy rate of 88 %. Providers would need to compile annual reports of the execution of detection orders, including error rates of the technology deployed and users' complaints, and of removal and blocking orders (with average time needed).

- Termination of voluntary detection

The proposed regulation does not envisage any transition regime between the Interim Regulation ending, and the entry into force of the new regulation, leaving a potential legal gap if it does not enter into effect on time.

**Privacy concerns of the European Data Protection Board and Data Protection Supervisor**

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted a Joint Opinion on the Proposal for a Regulation to prevent and combat child sexual abuse. The Proposal aims to impose obligations related to detecting, reporting, removing and blocking known and new online child sexual abuse material (CSAM), as well as the solicitation of children, on providers of hosting services, interpersonal communication services, software application stores, internet access services and other relevant services.

The EDPB and EDPS consider child sexual abuse as a particularly serious and heinous crime. Limitations to the rights to private life and data protection must, however, respect the essence of these fundamental rights and remain limited to what is strictly necessary and proportionate. The EDPB and EDPS consider that the Proposal, in its current form, may present more risks to individuals, and, by extension, to society at large, than to the criminals pursued for CSAM. Whilst supporting the goals and intentions behind the Proposal, the EDPS and EDPB express serious concerns about the impact of the envisaged measures on individuals' privacy and personal data. The lack of detail, clarity and precision of the conditions for issuing a detection order for CSAM and child solicitation **does not ensure** that only a **targeted approach to CSAM detection** will effectively take place. There is a **risk** that the Proposal could become the basis for a **generalised and indiscriminate scanning of content** of virtually all types of electronic communications. The EDPB and EDPS **advise that the conditions for issuing a detection order should be further clarified**.

**EDPB Deputy Chair, Ventsislav Karadjov, said:** *"There can be no doubt that child sexual abuse is a most abhorrent crime that demands swift and effective action, but the Proposal as it stands contains some serious shortcomings. It lacks legal certainty on multiple points and includes vague notions which may lead to diverging implementations across the EU, in particular regarding detection orders. As currently proposed, these orders may in fact even harm those they seek to protect. They could cause a substantial degradation of the confidentiality of communication, which would expose children using these services to monitoring or eavesdropping."*

In addition, the EDPB and EDPS are concerned about the **measures envisaged** for the detection of unknown CSAM and the solicitation of children in interpersonal communication services. The use of technologies to scan users' communications, such as artificial intelligence, are likely to generate errors, and represent a high level of intrusiveness into the privacy of individuals.

**EDPS Supervisor, Wojciech Wiewiórowski, said**: *"Measures allowing public authorities to have access to the content of communications, on a generalised basis, affect the essence of the right to private life. Even if the technology used is limited to the use of indicators, the negative impact of monitoring the text and audio communications of individuals on a generalised basis is so severe that it cannot be justified under the EU Charter of Fundamental Rights. The proposed measures related to the detection of solicitation of children in interpersonal communication services are extremely concerning."*

In their Joint Opinion, the EDPB and EDPS highlight that **encryption contributes in a fundamental way to the respect** of **private life and** to the **confidentiality of communications, freedom of expression**, innovation and growth of the digital economy. In particular, the EDPB and EDPS underscore the importance of end-to-end encryption, a commonly used tool that has strong technical and privacy safeguards. In light of this, the EDPB and EDPS make it clear that preventing or discouraging, in any way, the use of end-to-end encryption would seriously weaken the role of encryption in general.

A potential future EU Centre and a network of national Coordinating Authorities for child sexual abuse issues will be created under the new Proposal. The EDPB and EDPS welcome that this new structure will not affect the powers and competences of the data protection authorities. Nevertheless, the EDPB and EDPS **recommend that the relationship between the tasks of the national Coordinating Authorities and national data protection authorities are better regulated**. The Proposal should clarify the purpose, and process, for which the EDPB's Opinion on technologies used to execute detection orders may be requested.

On a similar note, the EDPB and EDPS take note of the envisaged close cooperation between the EU Centre and Europol, the EU's law enforcement agency combatting serious forms of crime. According to the Proposal, the two agencies' cooperation would involve the full access to relevant information systems of individuals' personal data, for the purpose of combatting child sexual abuse. Amongst several of their recommendations, the EDPB and EDPS recommend that instead of giving direct access to data, **transmitting personal data between the EU Centre and Europol** should **take place only on a case-by-case basis**, following a **thorough assessment of the request to access data in the information systems**, via a secure communication tool.

2 June 2023

MTÜ Inimiõiguste Teabekeskus