BRIEFING
EU Legislation in Progress

European Parliament

Combating child sexual abuse online

OVERVIEW

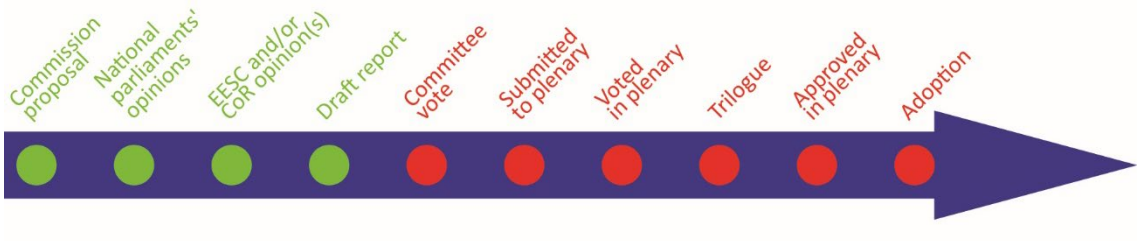
Online child sexual abuse materials (CSAM) and grooming (manipulative practices aimed at exploiting and abusing people), now increasingly targeting younger children, have been spreading at an alarming rate. In 2022, the more than 32 million reports of suspected online child sexual abuse, represented a historical peak. Among these reports, those on grooming marked an 82 % increase.

Most of the activities detected were hosted in Europe. In response to this situation, on 11 May 2022 the European Commission adopted a proposal for long-term rules to prevent and combat child abuse.

The Commission proposal would require interpersonal communication services, such as webmail messaging services and internet telephony, as well as others, to proactively detect online CSAM materials and activities involving child grooming. However, this poses many concerns regarding privacy, security and law enforcement investigations. The proposal also provides for the establishment of an EU centre to support the implementation and supervision of the new rules.

In the Parliament, the file has been assigned to the Committee on Civil Liberties, Justice and Home Affairs (LIBE). The draft report was submitted on 19 April 2023. The over 1 900 amendments tabled in committee were published on 30 May 2023.

Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse		
Committee responsible:	Committee on Civil Liberties, Justice and Home Affairs (LIBE),	COM(2022) 209 11.5.2022
Rapporteur:	Javier Zarzalejos (EPP, Spain)	2022/0155(COD)
Shadow rapporteurs:	Paul Tang (S&D, the Netherlands) Hilde Vautmans (Renew, Belgium) Patrick Breyer (Greens/EFA, Germany) Annalisa Tardino (ID, Italy) Vincenzo Sofo (ECR, Italy) Cornelia Ernst (The Left, Germany)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Committee vote	



EPRS | European Parliamentary Research Service

Author: Mar Negreiro
Members' Research Service
PE 738.224 – June 2023

EN

Introduction

In the past 20 years, the volume of online child sexual abuse materials (CSAM) has increased dramatically across the world aided by greater connectivity and technological development. The same is true of child grooming,[1] the practice of approaching children online to persuade them to produce sexual material of themselves and share it online, often in live streaming format. Not only is CSAM crime growing in scale but it is also growing more severe, as increasingly younger children are being exploited.

According to the US National Center for Missing & Exploited Children's (NCMEC) CyberTipline, over 32 million reports of suspected child sexual abuse online were received in 2022, making it a record year. Of these, 99 % were submitted by electronic service providers (ESPs), as defined by NCMEC. While CSAM was the largest category, there was an 82 % increase in reports on online enticement. NCMEC partially attributes this increase to financial sextortion. In early 2023, the US Federal Bureau of Investigation (FBI) issued a global warning about the rise in financial sextortion cases, where persons using fake accounts approach minors on digital platforms, coerce them into sending explicit photos or videos, and threaten to make these public unless the victim sends payment.

In 2022, 68 % of ESP-submitted CyberTipline reports were sourced from chats, messaging or email services within the European Union (EU). An additional 22 % of reports came from social media or online gaming platforms (which may also have integrated messaging or chat services), while the remaining 10 % came from the other listed platform types. According to the UK-based Internet Watch Foundation (IWF), 66 % of all known CSAM in 2022 was traced to an EU country.

Besides materials that have circulated on the internet for years and have already been identified or hashed, [2] CSAM now includes an increasing amount of new self-generated images and videos. When looking at the age groups, less than 2 % of reports mentioned children older than 13 years of age, while 98 % of reports mentioned children younger than that.

According to a 2022 report by the international hotline organisation INHOPE, self-generated content is on the rise even in the younger age groups. A majority of the victims featured in the 3-13 years category in 2022 had produced self-generated content.

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 underground paedophile networks. For instance, the UK's National Crime Agency estimates the number of people in the UK who pose a sexual threat to children at between 550 000 and 850 000.

Background

End-to-end (E2E) encryption systems can ensure the privacy and security of communications. This explains the general trend in recent years for online community forums, chat rooms and messaging apps to E2E encrypt their participants/members' communication exchanges. While providing a level of privacy and protection, E2E is also a safe haven for offenders. According to Europol, child sex offenders use defensive technical measures, including the anonymisation and encryption of their illegal online activities, to evade law enforcement, thereby hampering police investigations. Europol has found that CSAM distribution and sharing takes place on dark net forums, social networking platforms and E2E encrypted communication applications such as WhatsApp. This happens even though WhatsApp bans more than 300 000 accounts a month just from looking at their unencrypted parts. Some argue that technological development is advancing, with recent research papers outlining solutions for detecting CSAM within encrypted services.[3] Others, including the NCMEC, argue that if no way is found to detect CSAM within E2E encrypted services, the number of reports made could drop by as much as half. For that reason, in 2023 an international group of law enforcement agencies, including Interpol, the FBI, the Australian Federal Police and others, have been urging Meta – it being the leading global reporter of CSAM – not to introduce E2E encryption

on Facebook Messenger and Instagram. Others argue that E2E is here to stay, given its advantages for privacy and security, and that technologically realistic options should be considered

Existing situation

The EU has made the fight against child sexual abuse a priority in its 2020 EU strategy. In line with this strategy, the Commission set itself the goal to update in 2023 the related Directive 2011/93/EC (Child Sexual Abuse Directive) of 2011. The transposition of the directive into national law resulted in several shortcomings and fragmentation, which will need to be corrected.

The existing EU legislation to combat online CSAM, Regulation (EU) 2021/1232 (the Interim Regulation) provides for a temporary derogation[4] from certain obligations under Directive 2002/58/EC (the e-Privacy Directive), which protects the confidentiality of communications and traffic data.[5] The temporary derogation has enabled providers of number-independent interpersonal communications services to continue[6] their voluntary practices of detecting, reporting and removing child sexual abuse material online, since Directive (EU) 2018/1972 (on the European Electronic Communications Code) only entered into force at the end of 2020. This derogation will apply until 3 August 2024 or until an earlier date if the legislators do adopt the current proposal for a regulation and repeal this temporary measure.

In addition, the recently adopted Digital Services Act (DSA) is an important first step towards digital companies taking greater responsibility for content that appears on their platforms, including content related to children. The DSA requires the swift removal of illegal online content such as CSAM, illegal hate speech, terrorist content and illegal products. A growing number of platforms, including Tiktok and Facebook, are now training their moderators to detect these types of content.

Under the General Data Protection Regulation (GDPR), the processing of a child's personal data is considered lawful only if the child is 16 or older. When the child is under 16, such processing is lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility for the child. Member States' laws can provide for a lower age for those purposes, provided the lower age is not below 13 years. The majority of Member States have fixed an age that is under 16 years. However, social media platforms have limited possibilities to perform reliable age control checks. In many instances, parental control on social platforms does not come by default, in other words, it needs to be activated. That said, children are often able to bypass age barriers easily. For instance, according to its own terms and conditions relevant to the EU, WhatsApp is only open for use to persons older than 16. Yet, some studies show that much younger children in the EU use it regularly.

Parliament's starting position

Parliament has long been a strong advocate of securing a safer internet for kids, as well as defending privacy and data protection online.

For example, in its March 2021 resolution on children's rights in view of the EU strategy on the rights of the child, Parliament called on the Commission to develop an EU action plan for online service providers and tech companies to keep children safe online. It also highlighted the importance of digital literacy and education for children, regretting the existence of the digital divide that still hampers many children's safe access to digital technologies.

Council starting position

In its June 2022 conclusions on the EU strategy on the rights of the child, the Council called for the Member States to invest in reducing the digital divide. It also called for keeping a focus on privacy and online safety while also providing help for children who are victims of online abuse.

In its conclusions of 8 October 2019 on combating the sexual abuse of children, the Council recalled that the EU agenda on security lists cybercrime and all its ramifications, including sexual abuse and sexual exploitation of children, as one of the three main priorities to be addressed.

Preparation of the proposal

To accompany the proposal, the Commission did an impact assessment (IA) that drew on the input from a study and several consultations with a wide range of stakeholders.[7]

The Commission held a public stakeholder consultation from 11 February 2021 to 15 April 2021. It limited the consultation period to 9 weeks to be able to submit the initiative by the end of the second quarter of 2021, as planned in its 2021 work programme. Over 70 % of the 587 respondents[8] were EU citizens and about 10 % were NGOs. Over 45 % of respondents were from Germany.

The Commission launched two targeted surveys among law enforcement authorities with the goal to i) collect information on the state of play regarding the origin, quality and use of reports of child sexual abuse online; ii) collect information on the costs associated with reports of child sexual abuse online received by law enforcement authorities; iii) investigate how the quality of reports could be improved; and iv) assess the impact of encryption on investigations.

The Commission also did an inception impact assessment with a feedback period from 2 December 2020 to 30 December 2020. It received over 40 responses.

The Commission organised expert group meetings, workshops and other meetings.

Furthermore, three external studies were carried out in support of the IA.

The IA considered five policy options, labelled from A to E (including a non-legislative one), along with the baseline of no EU action.[9] According to the IA, the EU added value of the initiative lies in its potential to reduce the fragmentation of the internal market as well as providing legal certainty and a coherent approach.

The IA concluded that EU action is necessary (policy option E) to detect already known and new CSAM and to detect child grooming. According to the IA, without EU action, Member States would have to keep adopting national laws, which would likely lead to fragmentation and diverging laws.[10] The IA's preferred option includes the creation of an EU centre to coordinate the implementation of the new regulation.

The Commission's Regulatory Scrutiny Board (RSB) issued two opinions: a negative opinion on 16 June 2021 and a second marked 'positive with reservations' on 15 February 2022.[11]

For more information, see the related initial appraisal of the Commission's impact assessment, drafted by the European Parliamentary Research Service (EPRS).

The changes the proposal would bring

The Commission published its proposal on 11 May 2022.

The general objective of the proposal is to improve the functioning of the internal market (this is its legal basis) by introducing consistent mandatory EU rules to prevent and combat child sexual abuse online, covering both old and new CSAM as well as grooming.[12] This would be achieved notably by imposing detection, reporting and removal obligations on certain online service providers (mainly providers of hosting services and providers of interpersonal communication services, both referred to as 'providers').[13] Rules apply irrespective of the provider's place of establishment so long as it offers services in the EU. The three specific objectives of the proposal are to:

- ensure the effective detection, reporting and removal of online child sexual abuse (CSA);[14] this includes the dissemination of known or new CSAM and the grooming of a child;
- improve legal certainty, transparency and accountability and ensure protection of fundamental rights;
- reduce the proliferation and effects of child sexual abuse through harmonisation of the rules and increased coordination of efforts.

To improve coordination, the proposal provides for the establishment an EU centre on child sexual abuse (EUCSA) as a decentralised agency to enable the implementation of the new regulation. The key elements of the proposal are described below.

Risk assessment and mitigation

The proposal establishes a uniform mandatory obligation for all providers to assess the risk of misuse of their services for the dissemination of online CSA ('risk assessment'). This obligation also features in the recently adopted Digital Services Act (DSA).[15] Providers would be required to assess the risks associated with each of their services and include mitigating measures for these risks ('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 that may expose them to a high risk of grooming.

According to the Commission, mitigating measures would have the fundamental aim of protecting children from further circulation of images and videos showing their abuse and from being groomed into abuse. They would also allow service providers to potentially avoid being asked to draw up a detection order (see below), if their infrastructure is deemed to be robust enough to lower the risk of online CSA below a significant level. The EUCSA would create, maintain and operate databases of indicators for online child sexual abuse that providers would be required to use when making the assessment described in the previous paragraph.

National coordinating authorities (CAs)

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

Reports including the risks assessments and mitigating measures would need to be sent within 3 months to the CA and to the EUCSA. Within 3 months, the authority would have to review the reports and could require non-compliant providers to re-conduct or update the assessments or to introduce, review, discontinue or expand the mitigating measures within a period of up to 1 month.

Detection orders

The proposed legislation includes a detection order procedure.[16] If on looking at the risk assessment and risk mitigation analysis submitted by a provider the CAs come across evidence of a significant risk of misuse of a service, they would have to consider asking the provider to draw up a CSA detection order describing the specific risks they have identified. This would happen after considering whether the reasons for issuing the detection order outweigh the negative consequences for the rights and legitimate interests of all parties concerned. Before any detection order is issued, the service provider would have to be consulted. If the CA considers that the risks remain significant despite the mitigating measures, it could request a judicial or administrative authority to issue a detection order by using indicators that would be provided by the future EUCSA. The detection order would require the provider to deploy automated content recognition technologies to detect CSAM or grooming. The legislation leaves the choice of technologies to the provider concerned, provided that they meet the safeguarding requirements of the regulation: the proposal requires that the providers deploy technologies that are the least intrusive on privacy. Where potential detection involves high-risk processing, and for every case relating to the detection of grooming, the provider would have to 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 would have to 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 proposal provides a template and specifies that orders would have to include measures, indicators and safeguards. Orders would also have a set period of application. Providers would be

given at least 3 months and a maximum of 1 year to start the detection. Then providers would have to execute mandatory detection and report to the EUCSA any CSAM or grooming they detect or otherwise become aware of. Likewise, they would need to operate a system for users to flag potential child sexual abuse.

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, and it would also 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 relevant information society 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.

The competent law enforcement authorities would then 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 in question, 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 interference with activities on the prevention, detection, investigation and prosecution of child sexual abuse offences.

EU law and Court of Justice of the European Union (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 the right to challenge any measure affecting them. Users would 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 would 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, a sort of 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 would not need to perform any human oversight since the verification of the illegality of the CSAM would be done by the relevant authorities.

In contrast, considering the relatively high rate of false positive results for unknown CSAM and grooming, the proposal envisages that the detection of such material would require an additional degree of human oversight.[17] This opens up the question of how such human oversight is supposed to be organised on the side of providers.[18] For the detection of grooming, text-based pattern detection would be deployed. For one of these tools, Microsoft reports an accuracy rate of 88 %.

Providers would need to compile annual reports on the execution of detection orders, including error rates of the technology deployed and users' complaints, and on removal and blocking orders (with average time needed).

Termination of voluntary detection

The proposal does not envisage any transition period between the cessation of the Interim Regulation and the entry into force of the new regulation. This would leave a potential legal gap if the new regulation does not enter into force on time.

Advisory committees

On 22 September 2022, the European Economic and Social Committee (EESC) adopted an opinion on Combating child sexual abuse online package. The EESC supports the principle of the initiative, but highlights the risks to privacy and is sceptical about the scanning of encrypted communication. It considers the measures envisaged to be disproportionate and that there is a danger of the presumption of innocence to be infringed.

The European Committee of the Regions (CoR) has not taken any position on the issue.

National parliaments

The deadline for the submission of reasoned opinions on the grounds of subsidiarity was 14 October 2022. No reasoned opinions were submitted. Six political dialogues were put forward: by the Czech Chamber of Deputies, the Dutch Senate, the German Bundesrat, the Irish Houses of Oireachtas, the Portuguese Assembleia da República and the Spanish Cortes Generales. In addition there were two important 'information to exchange' documents filed by the Austrian National Council and the Czech Chamber of Deputies.

Stakeholder views[19]

On the whole, the proposal has been welcomed by stakeholders, but the discussion is polarised, notably with a view to possible disruptions of E2E encryption and interference with data protection and privacy, not least owing to the compulsory approach. Some organisations strongly support it, while others express strong criticism, mainly out of concern that the privacy of communications in E2E systems would be breached. Some also worry that the required user notifications might jeopardise ongoing investigations. Others also raise concerns about the potential administrative burden and compliance costs for SMEs, and ask for a targeted approach. Some providers favour a voluntary approach that would arguably enable current efforts and innovation. Many also ask for a clear transition period between the Interim Regulation and the new legislation to avoid legal gaps that might have a negative impact. For instance, during the 18 weeks between the entry into force of the European Electronic Communications Code (EECC) in December 2020 and the entry into effect of the temporary derogation from the e-Privacy Directive, there was a 58 % drop in files contained within EU reports to NCMEC.

Some would like interpersonal communication services designed for professionals and professional accounts to be excluded from the scope of the proposal. Others argue that livestream CSAM has unjustifiably been excluded from this scope. This could lead to criminal material shifting from one service to another (a wave effect). Yet others argue that the proposal is not consistent with EU law, among other things because of the provisions authorising the general monitoring of content online.

Selected stakeholder positions

In their joint opinion on the Commission proposal, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) expressed serious concerns, among them the fact that the proposal lacks clarity on key elements. Moreover, they found that the risk mitigation measures do not meet the legal certainty and foreseeability criteria needed to justify interference with the confidentiality of communications between private individuals. They therefore stressed that the proposal raises serious concerns about the disproportionality of the envisaged interference

and the limitations this interference places on the protection of fundamental rights, privacy and personal data protection.

Microsoft stated that no 'silver bullet' solution exists, and that therefore the proposed regulation should not impede online platforms' voluntary efforts. Rather, the regulation should reduce barriers to such efforts, including by 'deconflicting' other legal frameworks that offenders can exploit.

Google points out that current efforts across the EU to combat child sexual abuse and exploitation online are fragmented, duplicated, and/or insufficient in some areas, as shown in particular by the unsuccessful implementation of the Child Sexual Abuse Directive (Directive 2011/93). Google believes that a system that provides the right incentives for the detection of CSAM, together with a clear legal basis for personal data processing, should remain the framework for the detection, reporting and removal of child sexual abuse online. This system of voluntary measures should be complemented with a clear system of notice and takedown in accordance with the DSA framework.

UNICEF welcomes the proposal as an ambitious framework to address the violation of children's rights, and says that it is in line with Article 3(1) of the UN Convention on the Rights of the Child.

The Canadian Centre for Child Protection (C3P) highlights that almost half of Project Arachnid's removal notices had previously been flagged to the same hosting providers, which goes to show that providers are failing to use available technology to prevent the upload of known CSAM from being re-uploaded onto their services. They believe that regulation is long overdue and therefore support the proposed legislation. They also welcome the establishment of the EUCSA; this centre, in close collaboration with Europol, would facilitate the implementation of the rules.

The Global Encryption Coalition states that governments should preserve and promote E2E rather than compromise it. Governments should also encourage companies to engage in other activities that protect E2E. Governments should also promote solutions capable of addressing online harm and crime without undermining user privacy and security. For example, with regard to CSAM, they can encourage companies to facilitate the reporting of CSAM they have encountered and encourage the use of metadata analysis to better detect CSAM.

Cloudflare and the Interactive Software Federation of Europe for videogames (ISFE) insist that any proposal seeking to regulate the detection and removal of 'new' materials should consider the technical realities. They do not believe that it will be feasible to ask service providers to also track unknown CSAM, and they are not aware of technical solutions available to (cost-) effectively combat such materials, with human review likely to be both ineffective and conducive to a significant increase in the number of people having access to CSAM.

The International Association of Internet Hotlines (INHOPE) asks for five key aspects to be implemented to ensure that the proposed regulation can achieve its intended objectives: i) include official recognition of anonymous public reporting as a crucial element for detecting 'new or previously unidentified CSAM'; ii) develop a framework to facilitate legal recognition of EU hotlines so they can review, process, and potentially conduct pro-active searching for CSAM; iii) use existing and proven systems to avoid duplication and improve efficiency; iv) broaden the eligibility criteria to become a national CA to include already existing expert organisations; and v) develop a detailed framework to govern EUCSA partnerships with external organisations.

Missing Children Europe highlights that grooming, both online and offline, is a growing problem that exposes young people to the risk of becoming victims of sexual exploitation and trafficking, and potentially of going missing. They therefore welcome the inclusion of grooming in the category of offences qualifying as child sexual abuse and the introduction of the obligation for app stores to prevent children from downloading apps that present a high risk for grooming. They also call for more clarity on the conditions relating to the availability of technology provided free of charge. In particular, clarification is needed on whether the EUCSA will commit to covering 'reasonable' costs for maintenance and development, in addition to licensing for tools on its list, and how 'reasonable' will be defined, audited and reviewed for each technology and/or all items on the list.

ECPAT, an international organisation with 118 partner members in over 100 countries working to end child prostitution and child trafficking, stresses the importance of ensuring harmonised implementation of the proposed regulation to avoid the emergence of different standards across the EU. They propose that the regulation should include clearer obligations on the swift removal of CSAM as part of the recognition of victims' rights in order to limit potential re-victimisation. A survey of theirs shows broad EU citizens' support (68 %) for the use of tools to identify child sexual abuse materials, and for the EU to introduce long-term legislation that would keep children safe online.

Speaking from experience, NCMEC observes that far too many companies are not proactively fighting CSAM or that they engage in half-measures, decline to participate in voluntary initiatives, and often place organisational and financial concerns before child protection. By proposing more proactive and mandated measures to combat the proliferation of CSAM, the proposed regulation takes steps to address this situation. It fails however to indicate how the EUCSA would handle reports that have both an EU and a US nexus (e.g. relating to both EU and US offenders and/or victims). It lacks protocols for identifying and distinguishing reports relating to US offenders and/or victims and EU offenders and/or victims and how it would cooperate with key stakeholders in the US to process them. NCMEC also calls for reconsidering the notification requirements in the proposal in order to prioritise the safety of child victims. NCMEC also insists on the implementation of technological solutions that enhance consumer privacy while prioritising child safety with safeguards. NCMEC proposes to add a number of principles to safeguard children in E2E encrypted environments. Lastly, NCMEC warns that, to adhere with the proposed regulation, digital companies might have to send the same content twice to centres dealing with child sexual abuse material.

Two Leiden University academics, Dr Sabine K. Witting and Dr Mark R. Leiser, highlight that a key difference between 'known' and 'new' CSAM is that the classification of CSAM content is done outside a platform by an independent regulator or a law enforcement agency, before the hashing value is added to a distributed established database. For them it is crucial to point out that the technology deployed to detect new CSAM or grooming will not be able to differentiate between consensual sexual conversations or image sharing between two adolescents on the one hand, and unknown and un-hashed CSAM or grooming on the other hand. In a recent workshop with ECPAT, they provide recommendations to be used to discuss potential amendments in the proposal.

Zoom and the Information Technology Industry Council (ITI) say that the scope of the proposed regulation should only apply to interpersonal communication services used by consumers. Those designed and used in a professional context should be excluded.

The Dutch NGO, International Justice Mission (IJM), highlights that the proposed legislation omits to explicitly require detection, disabling, and reporting of livestreamed CSAM. IJM recommends that livestreamed CSAM be expressly included in the proposal, as children abused in livestreaming are in immediate danger of present and future harm and require identification and safeguarding.

The industry association Digital Europe has concerns about the interplay between the recently adopted DSA and the proposed regulation. They welcome the safeguards attached to detection orders, including judicial review, but state that these safeguards must be proportionate and offering effective protection to the privacy of all users. Detection orders must also be consistent with the ban on general monitoring, a principle that has recently been reconfirmed by the DSA. They express concern on the extension of the detection obligations to unknown CSAM material and grooming.

The Belgian App Association, representing thousands of small business software application development companies and technology firms, is against the proposal. Indeed, many App Association members currently do not register the ages of their users because they do not have a valid purpose for doing so, nor wish to take on the additional risk that holding such sensitive information entails.

The European Digital Rights Association (EDRi) highlights that the interpretation of new CSAM and grooming requires an analysis of the context that computers often fail to make. When the technology fails, legitimate freedom of speech is harmed, as are other fundamental rights, including

privacy. EDRi also reiterates that automated scanning and chat controls could indeed be illegal. This is further emphasised in a letter signed by EDRi and 117 organisations calling for tailored, effective, rights-compliant and technically feasible alternatives to tackle this grave issue.

Similarly, the German Lawyers' Association criticises the proposal in its position paper for being potentially harmful to fundamental rights, including privacy.

Legislative process

In the European Parliament, the file was assigned to the Committee on Civil Liberties Justice and Home Affairs (LIBE), with Javier Zarzalejos (EPP, Spain) as rapporteur. The following committees were invited to submit an opinion: the Committee on the Internal Market and Consumer Protection (IMCO), the Committee on Budgets (BUDG), the Committee on Culture and Education (CULT) and the Committee on Women's Rights and Gender Equality (FEMM).

On 10 October 2022, Commissioner Johansson presented the proposal to LIBE. Among other things, several MEPs questioned the operation and composition of the EUCSA, the place of current 'hotlines' in the new system, and the manner of interaction with the NCMEC's counterpart in the US.

In reply to the numerous questions on encryption during her hearing, the commissioner specified that the proposal does not mention 'encryption' and that only measures already in use should be applied, rather than techniques that are 'impossible' to put in place. The commissioner observed that the proposal ensures proportionality in a number of ways: through the involvement of all relevant stakeholders before any order is issued, the introduction of strict conditions and safeguards, and the involvement of a second independent authority. This rules out attempts at generalised and indiscriminate scanning of content for virtually all types of electronic communication.

CULT published its opinion on 29 March 2023. It supports the proposal and calls for an increased role for prevention measures, including digital skills, digital competence and media literacy.

LIBE asked the EPRS to draw up a complementary impact assessment that would focus on certain specific questions and critically review and complement the analysis, data and information contained in the Commission's IA. The complementary IA concluded that the overall effectiveness of the proposal is expected to be limited, among other things because the technology to detect new CSAM and grooming is not mature enough and that it would interfere with Articles 7 and 8 CFEU.

The draft report was published on 19 April 2023. The report welcomes and expresses support for the proposal's main aims, but also introduces numerous amendments (over 1 900, published on 30 May 2023). For instance, it incorporates search engines and other artificial intelligence systems in the scope of the proposal and limits CSA scanning in E2E encryption – done for the purposes of detecting suspicious patterns of behaviour without having access to the content of the encrypted communication – to metadata analysis.[20] It also creates a victims' consultative forum at the EUCSA and introduces the possibility for the continuation of voluntary CSA detection efforts in addition to the mandatory ones. It also reinforces prevention as part of the mitigating measures to be taken by providers; preventive measures include safety and security design for children by default, functionalities enabling age assurance and enhanced parental control tools allowing flagging and/or notifying mechanisms.

The rapporteur agrees that the rules should be laid down in a technology-neutral and future-proof manner, so as to encourage innovation. A key guiding principle of the report, aligned with the proposal, is compliance with the prohibition of a general monitoring obligation, this prohibition being enshrined in EU legislation and CJEU case-law. The rapporteur welcomes the safeguards introduced in the proposal. He also welcomes the EDPB-EDPS joint opinion, which he took into account in his report. The rapporteur supports the creation of the EUCSA. Regarding its seat, he aligns the provisions of the proposal with the recent ECJEU case-law.

Work at the Council is ongoing. The Czech Presidency of the Council is working on a compromise text on the proposed regulation.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Eisele K., Preventing and combating child sexual abuse, initial appraisal of a Commission impact assessment, EPRS, November 2022.

Eisele K. and Dalli H., Proposal for a regulation laying down rules to prevent and combat child sexual abuse, Complementary Impact assessment, study, EPRS, April 2023.

Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse. Targeted substitute impact assessment, Ex-ante Impact Assessment Unit, EPRS, 2021.

Mildebrath H., Squaring privacy rules with measures to combat child sexual abuse online, At a glance, EPRS, 2021.

Negreiro M., Online Age verification methods for children, At a glance, EPRS, February 2023.

Negreiro M., Curbing the surge in online child abuse, Briefing, EPRS, 2020.

OTHER SOURCES

Carr J., Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse, Council of Europe, 2019.

Europol, Internet Organised Crime Threat Assessment (IOCTA), 2021.

European Parliament, Combating child sexual abuse online 2022/0155(COD), Legislative Observatory (OEIL).

Internet Watch Foundation (IWF), 2021 annual report.

Teunissen C. and Napie. S., Child sexual abuse material and end-to-end encryption on social media platforms: An overview, Australian Government, July 2022.

US Congressional Research Centre, The Fourth Amendment and the Internet: Legal Limits on Digital Searches for Child Sexual Abuse Material (CSAM), March 2022.

Van der Hof S. and Ouburg S., 'We Take Your Word For It' — A Review of Methods of Age Verification and Parental Consent in Digital Services', *European Data Protection Law Review*, Vol. 8, 2022.

ENDNOTES

1 Grooming refers to a practice where child sexual abuse offenders build a relationship of trust with children so that they can manipulate and sexually exploit and abuse them.

2 Tech companies use hashing, PhotoDNA, artificial intelligence and other technology to recognise, remove and report online child sexual abuse.

3 Thoughts on Child Safety on Commodity Platforms, by Dr Ian Levy and Crispin Robinson, 21 July 2022.

4 The European Electronic Communications Code (EECC) entered into application in December 2020, bringing with it a new definition of electronic communications services. The new definition encompasses 'number-independent interpersonal communications services' (NI-ICS) such as webmail, chat services, and internet telephony providers. Correspondingly, the scope of the e-Privacy Directive and its transposition acts, which rely on the EECC's definition of electronic communications services, were automatically extended and now apply to NI-ICS. The explicit applicability of the e-Privacy Directive casts doubt on the compliance, as regards privacy, of voluntary NI-ICS practices involving the use of dedicated technologies to scan communications for child sexual abuse material in order to report and remove it. To accommodate these practices under the e-Privacy Directive, the co-legislators adopted a temporary derogation from the e-Privacy Directive, which is supposed to be replaced by the proposed regulation discussed in this briefing. These changes are without prejudice to the applicability of the GDPR, and the lawfulness and proportionality of such measures remains uncertain under the GDPR.

5 According to the related EPRS-commissioned target substitute impact assessment, the measures envisaged by the Interim Regulation constituted interference with the exercise of the fundamental rights to confidentiality of communications and protection of personal data.

6 This means than under the interim legislation, only those services that were detecting CSAM on a voluntary basis could continue doing it, whereas new providers wanting to start doing it are not allowed.

7 The dedicated consultation activities lasted 2 years, from February 2020 to January 2022. See IA, Annex 2, p. 133.

[8] Although the IA (p. 131) refers to 603 respondents, the European Commission webpage says 587.

[9] See intervention logic, p. 16 and Figure 3, p. 53 of the IA, on policy options.

[10] See IA, p. 41.

[11] Annex 1 of the IA outlines more broadly how the RSB recommendations were addressed.

[12] The identification of grooming only concerns interpersonal communications where it is known that one of the users is a child.

[13] Most of the provisions in the proposal apply to hosting service providers (e.g. social media, cloud and file sharing services, app stores) and providers of interpersonal communication services (e.g. messaging services and web-based e-mail services). However, a recital explains that the future regulation would also cover services that enable direct interpersonal and interactive exchange of information, even if they are a minor ancillary feature of another service (e.g. chats on gaming apps). Also some recitals apply to internet access providers (ISPs).

[14] In terms of definitions, the reference to CSAM builds on the relevant terms as defined in the 2011 Child Sexual Abuse Directive, namely, child pornography and pornographic performance, and aims to encompass all the material covered therein insofar as such material can be disseminated through the services in question (in practice, typically in the form of videos and pictures). Thus, it does not include web-streamed materials/live streaming. The definition is in line with the one contained in the current Interim Regulation. The same holds true in respect of the definition of 'solicitation of children' (or grooming) and 'online CSA'. For the definition of several other terms, the proposal relies on definitions contained in other pieces of EU law or proposals, in particular the EECC and the DSA.

[15] For instance, very large online platforms should be able to comply with Articles 3 to 6 of this proposal using a similar approach to compliance as the one applied as regards Articles 26 and27 of the DSA. Some stakeholders have called for consistency in the risk mitigation in both pieces of legislation, as otherwise different approaches might lead to legal uncertainty and a lack of clarity for companies. Reporting obligations for providers are also part of the DSA.

[16] As regards mandatory detection activities involving processing of personal data, the proposal (in particular the detection orders to be issued), uses Article 6(1)(c) GDPR (which provides for the processing of personal data that is necessary for compliance with a legal obligation under Union or Member State law to which the controller is subject) as the grounds for such processing. Therefore, unlike the Interim Regulation, the proposed regulation aims to explicitly provide mandatory detection, using Article 6(1)(c) GDPR as its legal basis.

[17] See Recital 28 and Article 10(4)(c) of the proposal.

[18] Note that Article10 of the proposal, entitled 'technologies and safeguards', provides safeguards for the technologies to be deployed but does not set safeguarding standards for human oversight and human intervention.

[19] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'

[20] According to the IA (p. 28), providers do not consider metadata an effective tool in detecting CSAM and it is usually insufficient to initiate investigations.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Second edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.