The Commission Proposal on Combatting Child Sexual Abuse

The Commission Proposal on Combatting Child Sexual Abuse - Confidentiality of Communications at Risk?

*Teresa Quintel**

I. Introduction

On 11 May 2022, the European Commission (Commission) issued a Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.[1] The proposed text aims at setting rules to effectively address the misuse of online services for purposes of child sexual abuse while providing robust safeguards.[2] For that purpose, the proposal lays down obligations on providers of relevant information society services to assess and minimise the risk that their services may be misused for online child sexual abuse, obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse and to remove or disable access to such material, and obligations on providers of internet access services to disable access to child sexual abuse material (CSAM).[3] Finally, the proposal establishes rules on the implementation and enforcement of the proposed provisions by national and EU authorities.[4] The proposal, and in particular the proposed new obligations on service providers, has met criticism due to the fear of a negative impact on privacy and data protection rights of individual users of online interpersonal communications services.[5]

The proposed Regulation is supposed to supplement the Digital Services Act with more specific provisions on child sexual abuse online[6] and follows the EU strategy for a More Effective Fight Against Child Sexual Abuse from July 2020[7]. In addition, the proposal aims at complementing a 2011 Directive on combating the sexual abuse and sexual exploitation of children and child pornography[8] and builds on the so-called Interim Regulation on combating online child sexual abuse[9]. The Interim Regulation is restricted to voluntary actions of a limited number of online services and applicable for a period of maximum 3 years.[10]

DOI: 10.21552/edpl/2022/2/13

* Teresa Quintel is Assistant Professor at the European Centre on Privacy and Data Protection (ECPC) at Maastricht University. For correspondence: t.quintel@maastrichtuniversity.nl.

1 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse', COM(2022) 209 final, Brussels, 11 May 2022.

2 European Commission Press Release, 'Fighting child sexual abuse: Commission proposes new rules to protect children'(Brussels, 11 May 2022), available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2976

3 Article 1(1)(a) to (d) of COM(2022) 209 final.

4 Article 1(1)(d) of COM(2022) 209 final.

5 Cf.: Iverna McGowan, 'Europe's online child abuse law will make us all less safe' (POLITICO, 29 June 2022), available at < https://www.politico.eu/article/europe-online-child-abuse-law-make-us-less-safe/?>; James Vincent, 'New EU rules would require chat apps to scan private messages for child abuse'(The Verge, 11 May 2022), available at <https://www.theverge.com/2022/5/11/23066683/eu-child-abuse-grooming-scanning-messaging-apps-break-encryption-fears> Natasha Lomas, 'Europe's CSAM scanning plan unpicked'(TechCruch, 11 May 2022), available at < https://techcrunch.com/2022/05/11/eu-csam-detection-plan/>, Mathieu Pollet, 'CSAM proposal: children first, privacy second?'(Euractiv, 27 May 2022), available at < https://www.euractiv.com/section/digital/podcast/csam-proposal-children-first-privacy-second/>; Edri, 'European Commission's online CSAM proposal fails to find right solutions to tackle child sexual abuse' (Edri.org, 11 May 2022) available at < https://edri.org/our-work/european-commissions-online-csam-proposal-fails-to-find-right-solutions-to-tackle-child-sexual-abuse/>.

6 European Commission (n 1).

7 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. EU strategy for a more effective fight against child sexual abuse, COM(2020) 607 final, Brussels, 24 July 2020.

8 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L 335/1. In particular for the definition of child sexual abuse offences, and on the Interim Regulation, in particular on its safeguards for the detection of online child sexual abuse, see: COM(2022) 209 final, 109.

9 The Interim Regulation lays down temporary limited rules to enable providers of certain communication services to use technologies for the detection, reporting and removal of online child sexual abuse on their services, thereby derogating from certain obligations laid down in Directive 2002/58/EC (ePrivacy Directive). See: Article 1(1) of Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance) [2021] OJ L 274/41.

10 COM(2022) 209 final, 108. The Interim Regulation will expire in August 2024. The Interim Regulation had been subject to an opinion by the European Data Protection Supervisor (EDPS) [EDPS Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online (10 November 2020)] in which the EDPS held that the measures under the Interim Regulation would constitute an interference with the fundamental rights to respect for private life and data protection of all users of popular electronic communications services (page 15, note 52).

According to the Commission, in 2021 alone, 85 million pictures and videos depicting child sexual abuse were reported worldwide, with a significantly higher number of unreported cases.[11] The Commission argues that, due to the lack of harmonised rules at EU level on the detection, reporting and removal of CSAM, service providers[12] face divergent requirements to tackle the dissemination of such material. Although providers would voluntarily employ technologies to detect, report and remove CSAM, these measures would vary widely and were proven to address the issue insufficiently. In addition to the insufficient nature of the measures, voluntary action by providers would no longer be likely once the Interim Regulation expires.[13]

The current proposal obliges providers of hosting services[14] and providers of interpersonal communications services[15] to assess and mitigate the risk of any misuse of their services for online child sexual abuse purposes. In cases where, after the implementation of mitigating measures, a residual risk would remain, providers could be ordered to detect[16], report, remove or block access to CSAM. National judicial authorities or other independent administrative authorities would, at the request of so-called Coordinating Authorities, issue such detection, removal and blocking orders. These Coordinating Authorities would be established in each Member State and would cooperate with their counterparts in the other Member States[17], national law enforcement authorities (LEAs) and a newly established EU Centre on Child Sexual Abuse (EU Centre).

In addition, the proposal obliges providers to report potential CSAM, which they become aware of, to the EU Centre.[18] In order to facilitate the detection, reporting and removal of CSAM, the EU Centre would analyse and review reports received from service providers and would forward such reports to national LEAs and Europol. In addition, the EU Centre would act as a hub of expertise to assist Member States regarding best practices on prevention and on assistance to victims.[19]

While providers shall not be held liable for CSAM on their services[20], the risk to lose their liability exemption, the proposal argues, will prompt providers to regularly choose to remove CSAM.[21] With regard to providers that do not have an establishment in the EU, the legal representative that is to be designated by those service providers may be held liable.[22] This would mean that, theoretically, providers would have to systematically scan all communication taking place on their services and report any potentially suspicious material to the Coordinating Authorities as well as to the EU Centre.

This contribution aims at providing a general overview of the main features of the proposal and points to some of the main concerns around the proposed rules, in particular with regard to the protection of personal data. For that purpose, Section 2 will illustrate the structure of the proposal, explain the

11 European Commission (n 1).

12 Such as social media platforms, gaming services, other hosting and online service providers.

13 European Commission (n 1).

14 Article 2(a) of the proposal defines hosting service as an information society service as defined in Article 2, point (f), third indent, of the proposed Digital Services Act, European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final, Brussels, 15 December 2020. The DSA Proposal states that a 'hosting' service that consists of the storage of information provided by, and at the request of, a recipient of the service as one of the services of an intermediary service.

15 Article 2(b) defines interpersonal communications service as a publicly available service as defined in Article 2, point 5, of Directive (EU) 2018/1972, including services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service. Directive (EU) 2018/1972 in turn defines interpersonal communications service as a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service. See: Article 2(5) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36.

16 Article 7 of COM(2022) 209 final.

17 For instance in cases where a Coordinating Authority that is not the Coordinating Authority of establishment has reasons to suspect that a provider of relevant information society services did not comply with its obligations under the proposed rules, it shall request the Coordinating Authority of establishment to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance. See: Article 37(1) of COM(2022) 209 final.

18 Article 12 of COM(2022) 209 final.

19 European Commission (n 1).

20 Article 19 of COM(2022) 209 final.

21 COM(2022) 209 final, 17.

22 Article 24(5) of COM(2022) 209 final.

procedure on the issuing of orders by Coordinating Authorities and address the governance model of the proposed Regulation. Sections 3 and 4 will exemplify some of the general concerns that arise and demonstrate several data protection issues related to the proposed rules.

II. Overview of the Proposal

1. Legal Basis and Scope of the Proposal

Being based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), the proposal aims at eliminating existing barriers to the provision of relevant services within the Digital Single Market while allowing for an effective fight against online child sexual abuse. For that purpose, the proposed Regulation introduces uniform obligations of risk assessment, mitigation and mandatory reporting to relevant authorities for all providers of hosting or interpersonal communication services offering such services in the EU's Digital Single Market. The scope of these obligations is supposed to cover providers offering services on the Digital Single Market regardless of where they have their principal establishment.[23]

The Legislative Impact Assessment for the proposal opted for an option that includes both the detection of known and new CSAM by service providers. Hence, on the one hand, providers would be required to detect material previously confirmed to constitute CSAM. On the other hand, providers would have to detect material that could potentially constitute CSAM, but which would not (yet) be confirmed as such by an authority.[24] In addition, service providers would be obliged to detect material that concerns the solicitation of children[25], which the proposal defines as so-called 'grooming'[26]. According to the proposal, the requirement to detect unknown CSAM and grooming would result in the identification of new victims and create a possibility for their rescue from ongoing abuse.[27]

2. The Six Chapters of the Proposal

Chapter I and II of the proposed text set out the scope and relevant definitions used in the proposal, contain the provisions that oblige providers to assess the risk of their services to be used for CSAM purposes, to implement mitigating measures and stipulate the reporting requirements to the relevant national authorities. In addition, the chapters stipulate the conditions regarding detection and removal orders and the situations in which providers shall disable access to CSAM. Finally, providers are required to independently detect CSAM and report it via the EU Centre.

Chapter III contains rules on the enforcement of the proposed rules by the national Coordinating Authorities, which may conduct searches, submit notices to service providers and receive complaints against the latter. Furthermore, the Chapter requires Coordinating Authorities to cooperate amongst each other, for instance, in form of joint investigations.

Chapter IV contains detailed provisions on the establishment of the EU Centre, which is to act as a dedicated reporting channel for the entire EU, receiving reports on potential online child sexual abuse from all providers of hosting or interpersonal communication services. In addition, the EU Centre is supposed to maintain and operate databases on indicators of CSAM and to closely work together with Europol.

Finally, Chapters V and VI of the proposal impose transparency and reporting obligations on service providers, the Coordinating Authorities as well as the EU Centre and contain the final provisions on the proposed Regulation's evaluation, delegated and implementing acts as well as the repeal of the Interim Regulation.

3. The Risk-Based Approach

The proposal obliges hosting or interpersonal communication service providers to carry out an assessment of the risk that their service could be used for the purpose of online child sexual abuse.[28] Under the

23 COM(2022) 209 final, 7.

24 COM(2022) 209 final, 10.

25 The crime of sexual solicitation of a child occurs when an adult solicits a child (under 18) to engage in a sexual act or uses a computer or electronic device to solicit a child to engage in sex.

26 The Cambridge dictionary defines grooming as the criminal activity of becoming friends with a child in order to try to persuade the child to have a sexual relationship.

27 COM(2022) 209 final, 14.

28 Article 3(1) of COM(2022) 209 final. Pursuant to Article 3(4) of the proposal, such risk assessment shall be carried out within three months after the entry into force of the regulation of by three months from the date at which the provider started offering the service in the Union.

proposed rules, service providers are obliged to identify, analyse and assess such risk for each service that they offer.[29] The risk assessment shall take into account any previous use of their services for online child sexual abuse purposes[30], policies on such risk[31], the manner in which the service is used[32] and operated[33], and the way in which the service may be used by different age groups of children and for the solicitation of children.[34] With regard to the latter, service providers shall take into consideration whether adult users may search child users, either directly or indirectly and if images and videos may be shared via private chats.[35] Software application stores shall, where there is a significant risk that any of their products may be used for the purpose of child solicitation, take reasonable measures to prevent children from accessing them.[36]

Following that assessment, providers shall, where risk has been identified, implement mitigating measures to minimize such risk in a customised manner.[37] In accordance with proposed Article 5, the results of the risk assessment and any mitigating measures shall be reported to the Coordinating Authorities in the Member States. The latter are supposed to be established as the primary national authorities for the consistent application of the proposed rules[38] and to be granted specific investigatory and enforcement powers.[39]

Where, after the implementation of mitigating measures, a residual risk remains, a provider may be ordered to detect CSAM on its services by the competent Coordinating Authority in the Member State where the provider is established.[40] In order to enable direct communication with relevant public authorities, service providers are supposed to establish a single point of contact[41] and, in cases where they are not established in the EU but offer their services in the Internal Market, a legal representative[42]. The risk assessment is to be carried out every three years or earlier in case the service provider was subject to a detection order[43] or where the risk has changed[44].

In addition to the above obligations, providers, when becoming aware of activity indicating potential child sexual abuse on their services, must submit a report to the EU Centre.[45] The report shall contain information such as all content data, including images, videos and text[46], all available data other than content data related to the CSAM[47], geolocation data such as IP addresses[48] or information concerning the identification of any user involved in the potential child sexual abuse[49].

4. Orders Requested by Coordinating Authorities

The Coordinating Authorities are, besides other national administrative authorities and national courts, supposed to assess the provided material or conversations in order to confirm that it constitutes online child sexual abuse. Under proposed Article 7, Coordinating Authorities would request the judicial authorities or other independent administrative authority in their Member State to issue detection orders against providers under their jurisdiction. Before requesting such orders to be carried out, the Coordinating Authorities are supposed to assess the evidence of risks of the service to be used for online child sexual abuse purposes, taking into consideration additional information provided by the EU Centre[50] and the provider itself. In a subsequent step, the Coordinating Authority would submit a draft request for a detection order to the provider and the EU Centre, which in turn would both have the opportunity to comment on the draft request.[51] If the Coordinating

29 Article 3(1) of COM(2022) 209 final.
30 Article 3(2)(a) of COM(2022) 209 final.
31 Article 3(2)(b) of COM(2022) 209 final.
32 Article 3(2)(c) of COM(2022) 209 final.
33 Article 3(2)(d) of COM(2022) 209 final.
34 Article 3(2)(e)(i) and (ii) of COM(2022) 209 final.
35 Article 3(2)(e) (iii) of COM(2022) 209 final.
36 Article 6 of COM(2022) 209 final.
37 Article 4(1) of COM(2022) 209 final.
38 Article 25 of COM(2022) 209 final.
39 Articles 27 to 30 of COM(2022) 209 final.
40 Article 7 of COM(2022) 209 final.
41 Article 23 of COM(2022) 209 final.
42 Article 24 of COM(2022) 209 final.
43 Article 3(4)(a) of COM(2022) 209 final.
44 Article 3(4)(b) of COM(2022) 209 final.
45 Article 12(1) of COM(2022) 209 final.
46 Article 13(1)(c) of COM(2022) 209 final.
47 Article 13(1)(d) of COM(2022) 209 final.
48 Article 13(1)(f) of COM(2022) 209 final.
49 Article 13(1)(g) of COM(2022) 209 final.
50 Article 7(2) and Article 7(4)(a) and paragraphs (a),(b),(c) and (d) of the second sentence of COM(2022) 209 final.
51 Article 7(3) of COM(2022) 209 final.

Authority, after receiving the comments from the provider and the EU Centre would uphold its view that the evidence for a significant risk of the service to be used for child sexual abuse persists, it would submit an adjusted request that would take into account the comments received by the provider and the EU Centre.

The provider would then be required to submit an implementation plan on how the detection order would be executed, indicating the technologies to be used and the safeguards to be provided. In certain cases, the provider would be required to carry out a data protection impact assessment (DPIA) and, depending on the results of the DPIA, the competent data protection authority (DPA) would have to be consulted.[52] In case the Coordinating Authority, after this procedure, would still be of the view that the significant risk of the service to be used for child sexual abuse remains, it would be able to request the national judicial authority or other independent administrative authority to issue a detection order.[53] Different conditions are to be respected with regard to assessing the risk of known and new CSAM[54] and the solicitation of children[55].

Pursuant to proposed Article 7, detection orders shall be targeted and specific, shall take into account only available detection technologies, be limited to parts of the component of a service, be accompanied by proportionate safeguards and be applied for a period strictly necessary for the execution of the order.[56] The maximum period of application for detection orders of known and new CSAM would be 24 months, while the duration for detection orders concerning the solicitation of children would be 12 months.[57] In addition, proposed Article 8 contains a list of information and details, which shall be included in a detection order.[58]

While the procedure on removal orders is less detailed, the procedure on blocking orders is similar to the one on detection orders, albeit including fewer authorities. Whereas removal orders may be requested by a Coordinating Authority after itself, a court or another independent administrative authority identified CSAM[59], orders to block access to known CSAM are based on indicators in the database held by the EU Centre and take into account the information presented by the provider[60]. Blocking orders may remain in place for a period of five years, must, however, be reviewed by the competent Coordinating Authority every 12 months.[61] All types of orders are to be submitted to the main establishment of the provider or its legal representative in cases where the provider is not established in the EU.

The results of the assessment of the CSAM by Coordinating Authorities in the Member States are to be submitted to the EU Centre via a dedicated system[62] and fed into the EU Centre's databases of indicators that shall facilitate the detection of known and new CSAM and material on the solicitation of children[63]. In addition, contact officers established within each Coordinating Authority who enjoy the privileges and immunities necessary for the performance of their tasks[64] are supposed to assist in the exchange of information between the Coordinating Authority and the EU Centre[65]. The Coordinating Authorities are supposed to cooperate at EU level[66] and may carry out joint-investigations, including with the assistance of the EU Centre[67].

The investigatory powers of the Coordinating Authorities include requiring service providers to provide information relating to CSAM[68], the power to carry out onsite inspections of any premises of providers in order to examine, seize, take or obtain

52 Article 7(3) paragraphs (a) and (b) of the second sentence of COM(2022) 209 final.

53 Article 7(3) last sentence of COM(2022) 209 final.

54 With regard to known CSAM, the conditions are stipulated under Article 7(5), the conditions relating to new CSAM are laid down in Article 7(6) of COM(2022) 209 final.

55 Article 7(7) of COM(2022) 209 final. In addition, detection orders concerning the solicitation of children shall apply only to interpersonal communications and where one of the users is a child user.

56 Article 7(8)(a) to (c) of COM(2022) 209 final.

57 Article 7(9) of COM(2022) 209 final.

58 When a detection order becomes final, the competent judicial authority or independent administrative authority that issued the detection order shall transmit a copy thereof to the competent Coordinating Authority. The latter shall then transmit a copy thereof to all other Coordinating Authorities through a dedicated system. See Article 9(2) of COM(2022) 209 final.

59 Article 14(1) of COM(2022) 209 final.

60 Article 16 of COM(2022) 209 final.

61 Article 16(7) of COM(2022) 209 final.

62 Article 36 of COM(2022) 209 final.

63 Article 44(1) of COM(2022) 209 final.

64 Article 52(3) of COM(2022) 209 final.

65 Article 52(2) of COM(2022) 209 final.

66 Article 37 of COM(2022) 209 final.

67 Article 38 of COM(2022) 209 final.

68 Article 27(1)(a) of COM(2022) 209 final.

copies of information relating to CSAM[69], to ask any member of staff or representative of those providers to give an explanation regarding CSAM[70] and the power to enquire with providers whether measures to execute a detection, removal or blocking were taken[71].

Pursuant to proposed Article 28, the enforcement powers of Coordinating Authorities include the power to make commitments by providers binding[72], the power to order the cessation of infringements of the proposed rules[73], the power to impose fines for infringements and non-compliance with orders[74], to impose a periodic penalty payment[75] and the power to adopt interim measures to avoid risks of serious harm[76].

Member States may grant additional investigatory and enforcement powers to the Coordinating Authorities.[77] Moreover, additional enforcement powers may be granted to Coordinating Authorities in situations where all other powers have been exhausted[78], where the infringement persists[79] and where the powers available to Coordinating Authorities are not sufficient to prevent serious harm[80].

5. The EU Centre on Child Sexual Abuse

Article 40 of the proposal establishes a new EU Agency[81] to prevent and combat child sexual abuse, the EU Centre on Child Sexual Abuse.[82] The EU Centre is supposed to support and facilitate the implementation of the proposed rules on the detection, reporting, removal or disabling of access to, and the blocking of CSAM. In addition, it shall gather and share information and facilitate cooperation between relevant public and private parties involved in the prevention and combating of online child sexual abuse.[83]

In accordance with Article 43 of the proposed Regulation, the main tasks of the Centre would be the facilitation of risk assessments, detection, reporting, removal and blocking processes, and facilitating the generation and sharing of knowledge and expertise. The Centre is supposed to assess reports on potential CSAM and to forward those reports that are not manifestly unfounded to Europol and competent national LEAs.[84] In addition, the EU Centre would, under certain circumstances, be allowed to conduct online searches for CSAM or to notify such material to the providers in order to request the removal or disabling of access based on the providers' voluntary consideration.[85]

Pursuant to proposed Article 44, the Centre is supposed to create and maintain databases of indicators of online child sexual abuse in order to detect the dissemination of both previously known[86] and previously unknown CSAM[87], as well as indicators to detect the solicitation of children[88]. These indicators would consist of digital identifiers[89], a list of uniform resource locators[90] and additional information[91]. The indicators would be generated by the EU Centre on the basis of CSAM identified by the Coordinating Authorities, the national courts or other independent authorities of the Member States.[92] Recital 56 of the proposal adds that the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre

69 [O]r to request other public authorities to do so, Article 27(1)(b) of COM(2022) 209 final.

70 Article 27(1)(c) of COM(2022) 209 final.

71 Article 27(1)(d) of COM(2022) 209 final.

72 Article 28(1)(a) of COM(2022) 209 final.

73 Article 28(1)(b) of COM(2022) 209 final.

74 [O]r request a judicial authority in their Member State to do so, Article 28(1)(c) of COM(2022) 209 final.

75 Article 28(1)(d) of COM(2022) 209 final.

76 Article 28(1)(e) of COM(2022) 209 final.

77 Article 27(2) and Article 28(2) of COM(2022) 209 final.

78 Article 29(1)(a) of COM(2022) 209 final.

79 Article 29(1)(b) of COM(2022) 209 final.

80 Article 29(1)(c) of COM(2022) 209 final.

81 Article 41(1) states that the EU Centre shall be a body of the Union with legal personality.

82 Article 40(1) of COM(2022) 209 final.

83 Article 40(2) of COM(2022) 209 final.

84 Article 48(3) of COM(2022) 209 final.

85 Article 49(2) of COM(2022) 209 final.

86 Article 44(1)(a) of COM(2022) 209 final.

87 Article 44(1)(b) of COM(2022) 209 final.

88 Article 44(1)(c) of COM(2022) 209 final.

89 Article 44(2)(a) of COM(2022) 209 final.

90 Article 44(2)(b) of COM(2022) 209 final.

91 Article 44(2)(c) of COM(2022) 209 final.

92 Article 44(3) of COM(2022) 209 final. Pursuant to Article 36(1) of the Proposal, the EU Centre would generate indicators based on specific items of material and transcripts of conversations that the Coordinating Authorities or the competent judicial authorities or other independent administrative authorities of a Member State have identified, after a diligent assessment, as constituting CSAM or the solicitation of children.

should also be allowed to bring certain material or conversations to the attention of the Coordinating Authorities for those purposes.

In addition, the EU Centre shall maintain and operate a database containing the reports submitted to it by providers of hosting services and providers of interpersonal communications services.[93] This database is supposed to contain the reports[94] as well as the Centre's decisions on whether a report was manifestly unfounded[95], whether it was forwarded to national LEAs or Europol[96] as well as additional information submitted by the provider or the Coordinating Authorities[97].

Article 46 of the proposal regulates access to databases held by the EU Centre, which would be granted to the Centre's staff[98] and, where necessary, the relevant providers[99], the Coordinating Authorities[100] and Europol[101]. Access would be granted upon the reception of a request, which would have to specify the purpose of the request, the modalities of the requested access, and the degree of access needed to achieve that purpose. In addition, the EU Centre would have to diligently assess requests and only grant access where it considers that the requested access is necessary for and proportionate to the specified purpose.[102]

III. General Concerns

The legal basis that was chosen for the proposed Regulation is Article 114 TFEU, the so-called 'internal market legal basis', which enables the co-legislator to adopt measures for the approximation of the provisions that have as their objective the establishment and functioning of the internal market. Nevertheless, according to the proposal, the measures contained in the proposed Regulation affect, in the first place, the exercise of the fundamental rights of the users of the services, in particular, the rights to respect for privacy and to the protection of personal data.[103] Only as an additional matter, the proposal names the freedom to conduct a business of the providers as fundamental right to be covered by the proposal that 'comes into play as well'.[104] Hence, the Commission recognizes that the proposed rules have a more noteworthy impact on users' fundamental rights to privacy and data protection than on providers' freedom to conduct a business.[105]

Although the steps that need to be followed in order to issue detection orders seem burdensome, depending on the national implementation and the authorities that will be designated to be Coordinating Authorities in the individual Member States, the issuance of such orders might turn out to be more straightforward than it appears in the proposal. Once such a detection order has been issued, it could remain in place for up to 24 months, which would mean that all communications of all users of interpersonal communication services could be scanned by detection technologies for a considerable time. Such general monitoring obligation of providers would have to be measures against the objective pursued by the measure and its effectiveness.

While the fight against online child sexual abuse is of utmost importance and would justify highly intrusive measures, the effectiveness of the proposed rules might not established in all cases: The majority of child abuse content is shared via platforms and forums, according to the board of directors of the child protection association in Germany.[106] In addition, identified and confirmed CSAM is often not deleted and remains online for a considerable time.[107] Therefore, the scanning of private messages on interpersonal communication services or e-mails could be seen as being neither proportionate nor effective.

The disproportionality of the proposal could be substantiated by the fact that already today, CSAM

93 Article 45(1) of COM(2022) 209 final.

94 Article 45(2)(a) of COM(2022) 209 final.

95 Article 45(2)(b) of COM(2022) 209 final.

96 Article 45(2)(c) of COM(2022) 209 final.

97 Article 45(2)(d) to (g) of COM(2022) 209 final.

98 Article 46(1) of COM(2022) 209 final.

99 Article 46(2) of COM(2022) 209 final.

100 Article 46(3) of COM(2022) 209 final.

101 Article 46(4) and (5) of COM(2022) 209 final.

102 Article 46(6) of COM(2022) 209 final.

103 COM(2022) 209 final, 12.

104 COM(2022) 209 final, 13.

105 Article 16 of the Charter of Fundamental Rights of the European Union.

106 Sören Brinkmann, 'EU-Gesetz gegen Kindesmissbrauchsinhalte: Chatkontrolle „nicht mit Menschenrechten vereinbar"', (Deutschlandfunk, 11 May 2022); available at https://www.deutschlandfunk.de/chatkontrolle-eu-messenger-kindesmissbrauch-scanning-durchsuchung-kommission-gesetzentwurf-100.html

107 Lutz Ackermann, Robert Bongen, Benjamin Güldenring and Daniel Moßbrucker, 'Ermittler lassen Bilder nicht löschen' (Tagesschau, 02 December 2021) available at <https://www.tagesschau.de/investigativ/panorama/kinderpornografie-loeschung-101.html>.

could be removed by other available means and from more relevant sources. In addition, the focus could be set on preventive measures, which would aim at detecting harmful behaviour by way of analysing metadata and preventing the dissemination of CSAM by banning certain users from accessing the relevant services. What is more, certain forums on which CSAM is being uploaded and shared will not fall within the scope of the proposal but would rather require political pressure on the countries hosting them.[108] Consequently, where CSAM could be identified by less intrusive means, the proposed rules would not satisfy the necessity requirement.

Finally, the proposal requires Coordinating Authorities to be legally and functionally independent from any other public authority, to act objectively and impartially, free from any external influence and not to be charged with tasks relating to the prevention or combating of child sexual abuse, other than their tasks under the proposed Regulation.[109] It remains unclear which authorities will assume the tasks of the Coordinating Authorities at national level. Since it is rather unlikely that new authorities will be created in the Member States, already established authorities will most likely serve as Coordinating Authorities.

The authorities in the Member States that would fulfil these requirements are courts or, in certain Member States, prosecutors or investigating judges.[110] With regard to the former, this would create a situation in which courts would request judicial authorities (other courts) to issue detection, removal and blocking orders. With regard to the latter, Member States could allow for situations in which a prosecutor would be enabled to request another prosecutor to issue a detection, removal or blocking order. In both scenarios, this would not only create structures in terms of competences and could lead to a conflict of interests, it also raises questions regarding the sufficiency of the legal basis of the proposal.

IV. Data Protection Concerns

As mentioned above, the proposal recognises that the measures contained in the proposed Regulation affect, in the first place, the exercise of the fundamental rights of the users of the services at issue. Those rights include, in particular, the fundamental rights to respect for privacy, to the protection of personal data and to freedom of expression and information.[111] While the freedom of expression and information is likewise affected by the proposed rules, this section will focus on the fundamental rights to privacy and data protection, which are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

1 Loss of Confidentiality of Communications

Since, the proposal encourages a 'technological neutral approach'[112] and does not suggest any specific filtering technologies to providers in order to enable them to carry out their monitoring obligations, it will be the responsibility of the providers to deploy the most effective and least intrusive tools to execute (detection) orders.

For the detection of CSAM, the proposal requires the operated technologies to identify the dissemination of known or new child sexual abuse material as well as behaviour indicating the solicitation of children.[113] These technologies shall be effective in detecting[114] while not be able to extract any other information from the relevant communications than the information strictly necessary to identify patterns pointing to the dissemination of known or new CSAM or the solicitation of children.[115]

Hence, the proposal requires the least intrusive measures in terms of the impact on the users' rights to private and family life, including the confidentiality of communication, and the protection of personal data.[116] In addition, the technologies shall be suf-

108 Vincent Först, 'Das sind Inhalte, die liegen außerhalb meiner Vorstellungskraft' (Netzpolitik.org, 09 May 2021), available at: <https://netzpolitik.org/2021/recherche-zu-paedosexuellen-foren-das-sind-inhalte-die-liegen-ausserhalb-meiner-vorstellungskraft/>.

109 Article 26(2)(a) to (e) of COM(2022) 209 final.

110 In addition, national DPAs would fulfill such a requirement.

111 COM(2022) 209 final, 12.

112 Recital 26 of COM(2022) 209 final states that in order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services.

113 Article 10(1) of COM(2022) 209 final.

114 Article 10(3)(a) of COM(2022) 209 final.

115 Article 10(3)(b) of COM(2022) 209 final.

116 Article 10(3)(c) of COM(2022) 209 final.

ficiently reliable, in that they limit to the maximum extent possible rates of errors regarding the detection[117] and providers should perform any necessary review on an anonymous basis and take steps to identify any user in case potential online child sexual abuse is detected.[118]

Consequently, it will be up to the providers to ensure that the technologies are effective while being the least intrusive and most reliable means to detect CSAM. The proposal leaves it entirely open *how* providers are supposed to detect CSAM on their services.[119] It therefore shifts the responsibility towards the provider to make the impossible possible: effectively detecting all CSAM while ensuring the security, the confidentiality of communication and the protection of personal data. How CSAM may be detected without abolishing end-to-end encryption of communications, however, remains unclear.

Known CSAM could be detected by way of hashing, which is a technique to make a search more efficient by effectively narrowing it down at the outset, using algorithms to map object data to a representative value.[120] With regard to new CSAM and cyber grooming, however, the content of communications would have to be scanned by other techniques. For unencrypted communications, scanning could take place during transfer. However, with regard to encrypted communication, the scanning of communication would have to take place directly on the device.[121] This would presumably require the removal of end-to-end encryption of communications. Evidently, this could also open possibilities for unauthorised access to communications, or the use of the detection technologies for the identification of additional types of illegal content in the future.

Detection orders are to be proportionate, limited in their duration and targeted in nature. However, where a residual risk remains, such an order could theoretically be continuously renewed and thus result in a permanent scanning of communications. Whether detection of CSAM may be carried out in a targeted manner is questionable, in particular, with regard to new CSAM or with regard to the solicitation of children.[122]

2. Accuracy of Detection Technologies

Because the detection process requires an automatic scanning of interpersonal communication content such as text, images and videos of users to identify CSAM and the solicitation of children, it is the most intrusive method for users.[123] An additional distinction needs to be made between the detection of known and new CSAM as well as grooming. As mentioned, while known CSAM may be detected by way of hashing, in order to identify new material, providers would have to use technologies that would scan communications and flag content that could depict CSAM. With regard to grooming, the employed technology would search for known, pre-identified patterns that would indicate *potential* grooming.

Generally, detection software that is available today and could be deployed to detect CSAM is not advanced enough to be reliably accurate and it is prone to generate false positives. This is particularly the case with regard to unknown or new CSAM and grooming. With regard to new or unknown material, the detection technology would have to identify never-before-seen images that constitute CSAM.[124] In certain cases, the detection technology could indicate a picture to depict CSAM while the content is absolutely harmless. An example one could imagine is a picture that would be shared in a private family chat, depicting a naked child within the family on the beach. The software could wrongfully detect CSAM and, in certain cases, such false positives could be forwarded to the national LEAs or the EU Centre and Europol.

According to the Commission, detection technologies to identify grooming acquired a high degree of accuracy in recent years. The proposal refers to Mi-

117 Article 10(3)(d) of COM(2022) 209 final.

118 COM(2022) 209 final, 7.

119 Recital 26 states that the proposed Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation.

120 'What is Hashing? How Hash Codes Work - with Examples' (FreeCodeCamp, 26 January 2020), available at <https://www.freecodecamp.org/news/what-is-hashing/>

121 Such as WhatsApp, Signal or Threema. Other communication that is not end-to-end encrypted, such as Facebook Messenger or E-mails, would be scanned during transfer.

122 Recital 23 proposes a limitation of the duration of application of the detection order that the Coordinating Authority deems necessary.

123 COM(2022) 209 final, 14.

124 Iverna McGowan, 'Europe's online child abuse law will make us all less safe' (POLITICO, 29 June 2022), available at <https://www.politico.eu/article/europe-online-child-abuse-law-make-us-less-safe/?>.

crosoft reports, which show that the accuracy of the grooming detection technology used by the cooperation is at 88%. According to the proposal, the remaining 12% would not be reported to law enforcement but could be excluded upon review.[125] However, this also means that out of 1 billion interpersonal messages, 120.000.000 conversations would have to be reviewed. Arguably, it is not possible to exclude that a certain part of these conversations would also be forwarded to the national LEAs, the EU Centre and Europol. The Commission argues that because of machine learning technologies, the indicators of grooming are becoming increasingly reliable, however, human oversight and review would remain necessary.[126] Whether such human oversight and review would be feasible is doubtful.

When looking at the amount of pictures being shared daily in the EU[127], this could lead to millions of alerts of suspicious CSAM where the actual content is harmless. Even if not shared with LEAs in all cases, a considerable number of different authorities, both at national and EU level, would be required to review and analyse or assess the flagged material. In cases where reports on child sexual abuse are not manifestly unfounded, those reports would indeed be shared with LEAs and Europol. How commonly such cases would materialize is unclear. However, in case of doubt, the likelihood that reports on potential CSAM would be forwarded for further analysis is rather high.

3. The EU Centre's Relationship with Europol

The relationship between the EU Centre and Europol is remarkable. For instance, the proposal argues that, in order to allow the EU Centre to achieve all of its objectives, it is of key importance that the EU Centre is established at the same location as Europol.[128] The proposal describes Europol as the EU Centre's closest partner[129] and suggests the Centre's seat to be in The Hague[130] in order to improve data exchange possibilities between the two Agencies, to create a knowledge hub on combatting CSAM and to rely on the support services of Europol.[131]

Pursuant to Article 53(2) of the proposal, Europol and the EU Centre shall provide each other with the fullest possible access to relevant information and information systems. In addition, and as mentioned above, the Centre shall forward the CSAM reports that are *not manifestly unfounded* to Europol for further analysis and subsequent referral by Europol to the competent LEAs.[132]

The processing of CSAM by Europol is worrying, in particular, in view of the recently adopted recast Europol Regulation[133], which allows the Agency to process personal data without separating data subjects into different categories.[134] This would mean that personal data of victims of child sexual abuse might be analysed together with personal data of perpetrators or suspects without defining specific access requirements or retention periods. In addition, the recast Europol Regulation substantiates the already questionable processing operations by the Agency, setting the focus on the analysis of large and complex data sets that allows Europol to *connect the dots* by way of matching data from different sources in one data environment.[135]

V. Conclusion

The proposed Regulation is a heavy piece of legislation that seeks to regulate in the smallest detail. For instance, the procedure on issuing detection, removal and blocking orders is highly complex, involving a multitude of authorities and appears to be rather burdensome. Hence, it could be argued that the threshold for issuing detection, removal and blocking orders is relatively high and requires the input from different actors that would need to be approved. Yet,

125 COM(2022) 209 final, 14.

126 COM(2022) 209 final, 14.

127 As example, in Germany alone, the number of sent WhatsApp messages in 2015 was 667 million. See: Statisa, 'Anzahl der verschickten SMS- und WhatsApp-Nachrichten in Deutschland von 1999 bis 2014 und Prognose für 2015', available at:<https://de.statista.com/statistik/daten/studie/3624/umfrage/entwicklung-der-anzahl-gesendeter-sms-mms-nachrichten-seit-1999/>.

128 COM(2022) 209 final, 11.

129 COM(2022) 209 final, 19.

130 Article 42 and page 4 of COM(2022) 209 final.

131 COM(2022) 209 final, 11.

132 Article 48(3) of COM(2022) 209 final.

133 Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation [2022] OJ L 169/1.

134 Cf. Teresa Quintel, 'The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation. The Question of Legitimizing Unlawful Practices', (April 2022) European Data Protection Law Review, Volume 8 (2022), Issue 1, p 90 – 102.

135 Ibid., 101.

depending on the authorities that the Member States will designate as Coordinating Authorities, the procedure might turn out to be less burdensome than it currently seems. In Member States where the prosecutor is deemed to be independent or in jurisdictions that foresee an investigative judge in their criminal procedure, issuing a detection order could be more straightforward.

In addition, it remains open how service providers will ensure that measures taken by them are the least intrusive, proportionate and accompanied with appropriate safeguards where they are ordered to permanently scan their services due to a residual risk of CSAM. The technologies used in order to detect CSAM are currently not sufficiently advanced in order to detect material in a reliable way and without a considerable error rate. In addition, the scanning for CSAM would not be possible without breaking the end-to-end encryption of communications. Another question that arises is whether preventative measures to tackle CSAM might be a more appropriate or supplementary option. For instance, the use of metadata to detect certain patterns on services and ban certain users from using them could be considered.

The most pertinent question that remains is the usefulness and necessity of the proposed measures: most CSAM takes place on forums, paedophile networks and on the dark-net or in the offline world. Where this is not taken into consideration, a significant part of child sexual abuse will remain at the status quo. An additional challenge is the fact that authorities often do not have sufficient resources and know-how in order to effectively tackle online child sexual abuse, which is an issue that the proposal cannot solve.

It is without any doubt that (online) child sexual abuse is one of the most horrific crimes and the generation and dissemination of CSAM as well as the solicitation of children online needs to be prevented, particularly in view of the drastic increase of such crimes in recent years. However, where more effective means are already known today and CSAM is more prominent elsewhere, the necessity of granting access by numerous national and EU authorities, including Europol, to material that is not CSAM should be very carefully considered. Exhausting the existing possibilities to detect and remove CSAM would protect the fundamental rights of millions of users, including children. This includes that individuals should be able to trust that their communications are not permanently monitored. Where even children's organisations[136] doubt the necessity and proportionality of the proposal, its added value remains questionable.

136 Süddeutsche Zeitung, 'Kinderschutzbund gegen anlasslose Kontrolle von Chats' (3 June 2022), available at < https://www.sueddeutsche.de/panorama/kriminalitaet-duesseldorf-kinderschutzbund-gegen-anlasslose-kontrolle-von-chats-dpa.urn-newsml-dpa-com-20090101-220603-99-538019>.