EXPERT WORKSHOP ON EU PROPOSED REGULATION ON PREVENTING AND COMBATTING CHILD SEXUAL ABUSE

jointly organized by the Center for Law and Digital Technologies (eLaw) of Leiden University and ECPAT International

Leiden University, 17th & 18th October 2022

OUTCOME REPORT

Prepared by:

Dr Sabine K. Witting, Assistant Professor for Law & Digital Technologies at Leiden University

Dr Mark R. Leiser, Assistant Professor for Digital, Internet Law, and Platform Regulation at VU-Amsterdam

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This Expert Workshop on the EU Proposed Regulation on Preventing and Combatting Child Sexual Abuse was jointly organized and funded by Leiden University and ECPAT International.

We would like to thank the Council of Europe for the technical and financial support provided to this workshop and its outcome report.

Special thanks to Amy Crocker, Isaline Wittorski, and Gioia Scappucci for their helpful comments, edits, and suggestions. The organizers also thank Li-Ru Hsu for notetaking throughout the duration of the workshop.

DISCLAIMER

The opinions expressed in this report are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe.

ABBREVIATIONS

AR	Augmented Reality
CJEU	Court of Justice of the European Union
CRC	United Nations Convention on the Rights of the Child
CRC Committee	United Nations Committee on the Rights of the Child
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
DSA	Digital Services Act
EDPS	European Data Protection Supervisor
EU	European Union
EUROPOL	European Union Agency for Law Enforcement Cooperation
E2EE	End-to-end encryption
IAs	Independent Authorities
NIICS	Number-Independent Inter-Personal Communication Services
PET	Privacy enabling technology
TFEU	Treaty on the Functioning of the European Union
URL	Uniform Resource Locators
VR	Virtual Reality

DEFINITIONS

The definitions below are taken from the 2022 EU proposed Regulation laying down rules to prevent and combat child sexual abuse[1] (hereafter 'proposed Regulation'). Any articles cited in the below definitions are those of the proposed Regulation. Directive 2011/93/EU refers to the Directive on combating the sexual abuse and sexual exploitation of children and child pornography (hereafter 'CSA Directive')[2]:

Child	means any natural person below the age of 18 years.
Child sexual abuse material	means material constituting child pornography or pornographic performance as defined in Article 2, points (c) and (e), respectively, of Directive 2011/93/EU.
Child sexual abuse offences	means offences as defined in Articles 3 to 7 of Directive 2011/93/EU.
Known child sexual abuse material	means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (a) of the proposed Regulation.
New child sexual abuse material	means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (b) of the proposed Regulation.
Online child sexual abuse	means the online dissemination of child sexual abuse material and the solicitation of children.
Solicitation of children	means the solicitation of children for sexual purposes as referred to in Article 6 of Directive 2011/93/EU.

[1] 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, 11.5.2022.
[2] Directive 2011/93/EU of the European Parliament and the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011.

1. INTRODUCTION

On 11 May 2022, the European Commission (hereafter 'Commission') published its proposed Regulation laying down rules to prevent and combat child sexual abuse [1] (hereafter 'proposed Regulation'). The proposed Regulation aims to establish a clear and harmonized legal framework to better identify, protect and support victims of child sexual abuse (hereafter 'CSA'), notably through a clarification of the rules and responsibilities of online service providers when it comes to online CSA. It seeks to provide legal certainty to providers as to their responsibilities to assess and mitigate risks and, where necessary, to detect, report and remove known child sexual abuse material (hereafter 'CSAM'), new CSAM or solicitation of children on their services in a manner consistent with the fundamental rights laid down in the Charter of Fundamental Rights of the European Union (hereafter 'EU Charter')[2], and as general principles of EU law. The proposed Regulation has solicited responses from a wide range of stakeholders and was strongly praised and heavily criticized alike. Some see the proposed Regulation as a crucial step to hold the private sector accountable for their role in responding to online CSA taking place on their platforms and services, while others regard the proposed Regulation as a trojan horse that introduces 'mass surveillance' across the EU.

The proposed Regulation forms part of the EU Commission's wider commitment to combat online child sexual abuse. This commitment encompasses the EU Strategy on the Rights of the Child (2021 – 2024)[3], the EU strategy for a more effective fight against child sexual abuse (2020 – 2025)[4] and the EU Better Internet for Kids (BIK+) Strategy (2022)[5]. In the EU strategy for a more effective fight against child sexual abuse, the Commission's priorities, amongst other prevention and response measures, are the development and implementation of strong legal frameworks to protect children from abuse and exploitation. This includes the implementation and revision of the Child Sexual Abuse and Exploitation Directive[6] (Hereafter the 'CSA Directive') adopted in 2011. This Directive sets minimum standards for EU Member States regarding prevention and response to child sexual abuse and exploitation online and offline, focusing on the criminalization of the various forms of child sexual abuse and exploitation across EU Member States. While this Directive only touches upon the responsibility of private sector companies in its Art 25 ('Measures against websites containing or disseminating child pornography'), the Commission envisaged separate regulatory pieces specifically zooming in on the role of private sector companies.

Against this background, the Commission proposed two legislative interventions regarding the detection of online CSA by private sector companies, with the former being of a temporary nature and the latter, the proposed Regulation, providing for a long-term, comprehensive legislative solution. To allow for the continuation of voluntary detection practices, the legality of which was challenged

[1] 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, 11.5.2022.
[2] European Union: Council of the European Union, Charter of Fundamental Rights of the European Union (2007/C 303/01), 14 December 2007, C 303/1.
[3] EU Strategy on the Rights of the Child (2021 – 2024), COM/2021/142 final.
[4] EU Strategy for a more effective fight against child sexual abuse (2020 – 2025), COM(2022) 212 final, 11.5. 2022.
[5] EU Better Internet for Kids (BIK+) Strategy (2022), COM(2022) 212 final, 11.5. 2022.
[6] Directive 2011/93/EU of the European Parliament and the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011.

following legislative changes, the EU Commission initially proposed a temporary derogation from certain rights and obligations under the 2002 e-Privacy Directive[7] (hereafter 'e-Privacy Directive') for the sole purpose of detecting and reporting CSA and removing CSAM. This 'Interim Regulation'[8] entered into force on 2 August 2021 and ceases to apply three years after its entry into force (3 August 2024). Second, the EU Commission proposed a Regulation which aims to replace the Interim Regulation and uses it as a reference to present a long-term framework that maintains some of the elements put forth under the Interim Regulation, while adding further obligations and mechanisms and covering a wider range of services, including private communications. Important standards for the rights, support, and protection of victims of crime such as online CSA are also set forth in the 2012 Victims' Rights Directive.[9]

These regulatory measures need to be aligned with a wide range of existing EU legislation, which directly or indirectly impacts the detection of online child sexual abuse on online platforms. This includes EU law focusing on the legal responsibility of platforms for their content, and subsequent actions required to prevent such services from being used for criminal offences. Important to mention in this context are the e-Commerce Directive[10] and the Digital Services Act[11] (hereafter 'DSA'). The proposed Regulation is conceptualized as a *lex specialis* to the general framework provided for by the DSA.[12] Further, the proposed Regulation needs to align with legal frameworks such as the e-Privacy Directive, which concerns the processing of personal data and the protection of privacy in the electronic communications sector. Equally important is the 2018 General Data Protection Regulation (hereafter 'GDPR')[13], which lays down rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data.

Most importantly, the proposed Regulation must be in conformity with the EU Charter, such as the prohibition of torture and inhuman or degrading treatment or punishment (Art 4 EU Charter), respect for private and family life (Art 7 EU Charter), protection of personal data (Art 8 EU Charter), freedom of expression and information (Art 11 EU Charter), freedom to conduct business (Art 16 EU Charter), non-discrimination (Art 21 EU Charter) and the rights of the child (Art 24 EU Charter).

---

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[8] 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 2022/58/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, COM(2020) 568 final, 10.9.2020.

[9] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA.

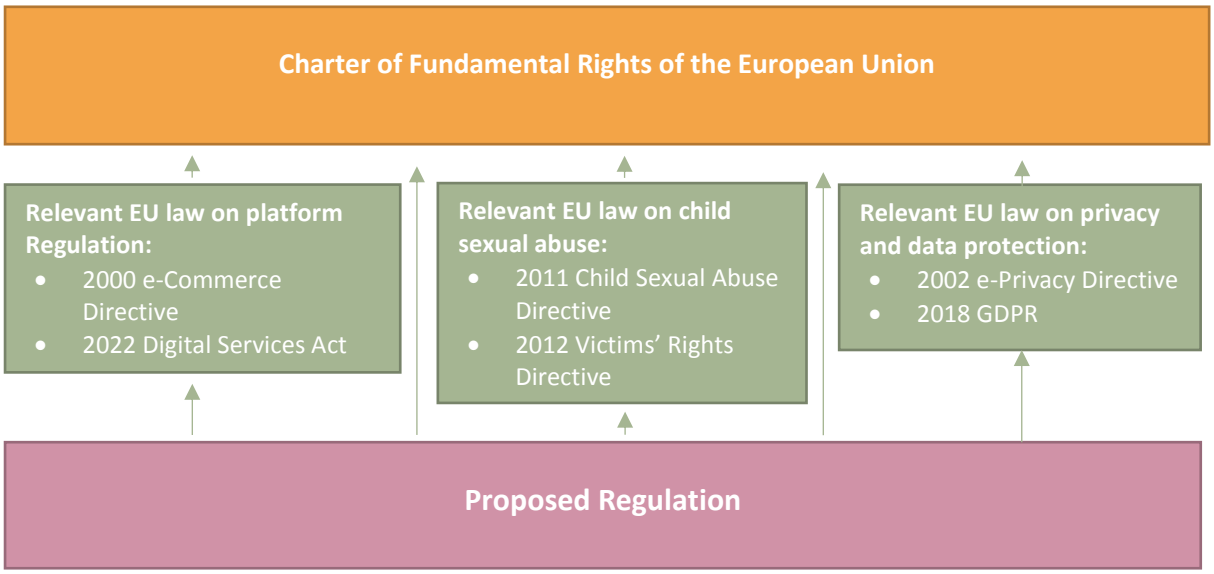
[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[12] See p. 5 proposed Regulation.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The below illustration demonstrates the relationship of the proposed Regulation with existing EU law and the EU Charter:



Lastly, it must be acknowledged that fighting online CSA cannot be achieved in a 'regional silo.' The proposed Regulation, if adopted, will impact law and policy making even beyond EU borders and should hence be assessed within the bigger picture of children's rights frameworks. This includes in particular the UN Convention on the Rights of the Child (hereafter 'CRC')[14], the CRC's Optional Protocol on the sale of children, child prostitution and child pornography[15] and the CRC Committee's General Comment No. 25[16], as well as the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms[17] (also known as 'European Convention on Human Rights') and the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse[18] (also known as 'Lanzarote Convention'). These international instruments provide important benchmarks for protecting children from online CSA at the global and regional levels and are considered important to be borne in mind in the context of the discussion on the proposed Regulation.

[14] UN Convention on the Rights of the Child, adopted and opened for signature, ratification, and accession by General Assembly resolution 44/25 of 20 November 1989.
[15] United Nations General Assembly, *Optional Protocols to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict and on the Sale of Children, Child Prostitution and Child Pornography* A/RES/54.263 (25 May 2000).
[16] CRC Committee, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, adopted on 24 March 2021.
[17] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.
[18] Council of Europe, *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual abuse*, 12 July 2007, CETS No.: 201.

2. WORKSHOP OBJECTIVES AND METHODOLOGY

Considering the impact of the proposed Regulation on fundamental rights laid down in the EU Charter, it is crucial to establish a proportionate balance between measures to protect victims of CSA and their fundamental rights, and users[19] (both adults and children) and their fundamental rights. This often leads to an extremely polarized discussion; for example, with some children's rights advocates defending such measures as necessary to keep children safe online on the one side, and some privacy advocates calling such measures 'mass surveillance' on the other. Such polarized positions risk distracting from the complexity of the debate and hinder thoughtful fundamental and child rights-based policy decisions.

When setting the objective of this workshop, representatives of Leiden University, VU-Amsterdam, and ECPAT International agreed that it is of utmost importance to create a mutual understanding of the various positions to create a fertile ground for a holistic, rights-based dialogue. Traditionally, the 'child rights' and the 'privacy' sectors have not had significant thematic overlap, leading to the impression that these interests are opposing and, thus, non-reconcilable. However, privacy and safety should be considered independent and interrelated rights that benefit from each other's strength: high privacy standards will positively impact children's safety, just as ensuring children's safety can positively impact safety and privacy standards for all.

Against this background, representatives of Leiden University, VU-Amsterdam, and ECPAT International brought together leading technical experts from various fields relevant for this workshop, including child rights, privacy and data protection, fundamental rights, and platform regulation. This approach was notably inspired by the Council of Europe's Independent Experts' Report issued to contribute to the discussions raised with respect to the Interim Regulation's negotiation.[20] This report indeed also aimed at capturing the perspectives of experts in the fields of human rights, child protection, data protection and cybercrime to offer possible ways forward respecting the various fundamental rights involved.

The workshop pursued the following objectives:

- to discuss the proposed Regulation from an issue-based perspective, zooming in on the most contentious topics of the debate; and
- to create a platform for constructive dialogue amongst the multi-sectoral experts which assists in forming a legal assessment of the proposed Regulation which achieves a proportionate balance between the various fundamental rights affected.

Pursuing idea sharing, awareness raising of the diversity of realities and professional expertise, this workshop was conceptualized from a problem-solving mentality which aims to deliver concrete outcomes and solutions, while allowing for sufficient time for critical analysis. Considering the sensitivity of the subject matter, the workshop was held under Chatham House Rules, meaning that participants were free to use the information received, but neither the identity nor the affiliation of

[19] Art 2 (h) proposed Regulation defines user as 'any natural or legal person who uses a relevant information society service'.

[20] Council of Europe, *Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse*, June 2021.

the speaker(s), nor that of any other participant, would be revealed. Accordingly, this report does not reveal the identity of any participants or the entities they represent.

To facilitate issue-based, substantive analysis and discussion, participants were asked before the workshop to prioritize thematic areas of the proposed Regulation they would like to discuss and debate in the workshop. These topics were prioritised by participants, and formed the core of the workshop and this outcome report:

1. Prohibition of general monitoring (see section 4.1);
2. Proportionality of proposed Regulation (see section 4.2);
3. Consensual online sexual exploration amongst adolescents (see section 4.3);
4. Continued voluntary detection of online CSA (see section 4.4).

However, other topics came out through the discussion which also provided important reflections on related subject matters (see section 5.1). Further, the workshop aimed to establish common ground on the discussed thematic areas of the proposal. Section 5.2 describes common ground identified during the workshop and other areas which require further interrogation and deliberation.

3. BRIEF SUMMARY OF THE PROPOSED REGULATION

Before diving into the workshop content, this section provides a brief overview of the proposed Regulation, with a focus on risk mitigation and detection orders, reporting, removal and blocking obligations and the proposed EU Centre. Please note that the below is a summary of the key aspects of the proposed Regulation and has been simplified to improve readability and accessibility.

3.1 RISK MITIGATION AND DETECTION ORDERS

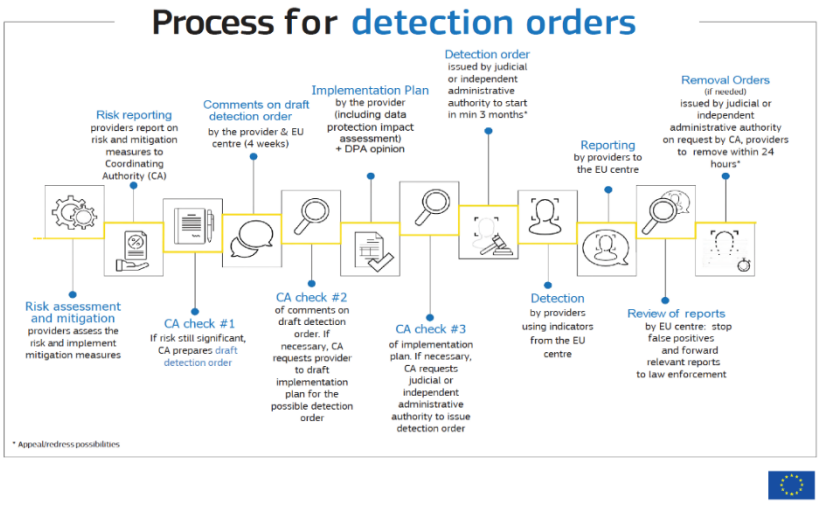
The proposed Regulation requires certain service providers[21] to identify, analyse and assess the risk of use of the service for the purpose of online CSA.[22] Following a risk assessment, those service providers are obliged to take reasonable mitigation measures, tailored to the identified risk. These may include adapting the provider's content moderation or recommender system, reinforcing internal processes, or initiating cooperation with other service providers.[23] The mitigation measures have to be effective, proportionate and targeted in relation to the risk identified, and applied in a diligent and non-discriminatory manner.[24] If providers of interpersonal communication services identify a risk of solicitation of children via services found on their platforms, they shall take necessary age verification and age assessment measures to reliably identify children on their services to allow for targeted mitigation measures.[25] For transparency purposes, the service provider shall clearly enunciate in their terms and conditions the mitigation measures they have taken.[26] Service providers must report the process and the result of the risk assessment as well as any risk mitigation measures to the Coordinating Authority.[27] The Coordinating Authority then determines whether the risk assessment and the risk mitigation measures meet the requirement set out in the proposed Regulation.[28]

A Coordinating Authority can request for a competent judicial or administrative authority to issue a detection order requiring the service provider to take measures to detect online CSA on a specific service.[29] A detection order can only be requested and issued if there is evidence of a significant risk of the service being used for the purpose of online CSA and the reasons for issuing a detection order outweigh negative consequences, in particular, ensuring a fair balance between affected fundamental rights.[30] The definition of the term 'significant risk' hereby depends on the type of CSA which is the object of the detection order. A significant risk concerning the dissemination of *known* CSAM exists where it is likely that the service is used, to an appreciable extent, for the dissemination of known child sexual abuse material and there is evidence that the service has been used, to an appreciable

[21] Providers of hosting services and providers of interpersonal communication services, see definition of these terms in Art 2 proposed Regulation.
[22] Art 3 proposed Regulation.
[23] Art 4 (1) proposed Regulation.
[24] Art 4 (2) proposed Regulation.
[25] Art 4 (3) proposed Regulation.
[26] Art 4 (4) proposed Regulation.
[27] For more information on the Coordinating Authorities for child sexual abuse issues, see Art 25 proposed Regulation.
[28] Art 5 (2) proposed Regulation.
[29] Art 7 (1) proposed Regulation.
[30] Art 7 (4) proposed Regulation.

extent, in the past 12 months for the dissemination of known child sexual abuse material.[31] The term 'appreciable extent' is hereby defined as 'beyond isolated and relatively rare instances'.[32] Regarding *new* CSAM, a significant risk exists if it is likely that the service is used, to an appreciable extent, for the dissemination of new CSAM; if there is evidence of the service having been used, to an appreciable extent, in the past 12 months for the dissemination of known child sexual abuse material; and if a detection order concerning the dissemination of known CSAM has been issued or the provider submitted a substantial number of reports concerning known CSAM.[33] And lastly, a significant risk relating to the solicitation of children exists if the provider qualifies as a provider of interpersonal communication services; if it is likely that the service is used, to an appreciable extent, for the solicitation of children; if there is evidence of the service having been used in the past 12 months and, to an appreciable extent, for the solicitation of children. It is important to add that the detection order regarding solicitation of children shall apply only to interpersonal communications where one of the users is a child user.[34]

When requesting the issuance of a detection order, the Coordinating Authority has to target and specify it in such a manner that any negative consequences remain limited to what is strictly necessary to effectively address the significant risk, for example by limiting the detection order to an identifiable part or component of the service or by adding additional safeguards.[35] In the same vein, detection orders should be limited in their duration to what is strictly necessary, with detection orders for known and new CSAM running up to 24 months, and for solicitation of children up to 12 months.[36] Providers and users affected by the measures have the right to effective redress, including the right to challenge the detection order before the courts of the Member State of the authority which issued the detection order.[37] A flow chart summarizing the process for the issuing of a detection order as described in the proposed Regulation follows:



[31] Art 7 (5) proposed Regulation.
[32] Recital 21, proposed Regulation.
[33] Art 7 (6) proposed Regulation.
[34] Art 7 (7) proposed Regulation.
[35] Art 7 (8) proposed Regulation.
[36] Art 7 (9) proposed Regulation.
[37] Art 9 proposed Regulation.

3.2 REPORTING, REMOVAL AND BLOCKING

The proposed Regulation further provides for provisions regarding reporting, removal and blocking of CSAM. A Coordinating Authority may request the competent judicial authority or another independent administrative body to issue a removal order to a hosting service, asking for removing or blocking access to identified CSAM. Coordinating Authorities, courts or other administrative bodies are thereby authorized to assess and identify content as CSAM. [38] Removal orders must be executed within 24 hours.[39] Providers of hosting services issued with a removal order and users who provided the material have the right to effective redress.[40]

Further, a Coordinating Authority may request the competent judicial authority or another independent administrative body to issue a blocking order requiring a provider of internet access services to prevent users from accessing known child sexual abuse material indicated by uniform resource locators (URLs) as included in the EU Centre's database.[41] Before issuing a blocking order, the Coordinating Authority must carry out an investigation and assessment to determine whether the criteria for issuing a blocking order have been met. This requires that there is evidence of the service having been used during the past 12 months, to an appreciable extent, for accessing CSAM as indicated by the URL; the blocking order is necessary, taking into account to the quantity and nature of the material, the URL indicates, in a sufficiently reliable manner, CSAM; and the reasons for issuing the blocking order outweigh negative consequences for rights and legitimate interests for affected parties. [42] Blocking orders must be limited in time and not exceed five years, with an obligation for the Coordinating Authority to assess any substantial changes for the ground of issuing the detection order at least once every year.[43] Affected providers of internet access services and users who provided or were prevented from accessing a blocked item have the right to effective redress.[44]

3.3 ROLE AND RESPONSIBILITIES OF THE EU CENTRE

To support the implementation of the proposed Regulation, the EU Centre will be established as an independent body of the Union with legal personality. [45] The EU Centre will facilitate the risk assessment, detection, reporting and removal processes. A central task is the creation, maintenance, and operation of databases of indicators of online CSA, which providers must use to comply with the detection orders. The EU Centre will also make technologies available for providers of the execution of detection orders. Further, the EU Centre will assist competent national authorities in the

[38] Art 14 (1) proposed Regulation.
[39] Art 14 (2) proposed Regulation.
[40] Art 15 proposed Regulation.
[41] Art 16 (1) proposed Regulation.
[42] Art 16 (4) proposed Regulation.
[43] Art 16 (7) proposed Regulation.
[44] Art 18 (1) proposed Regulation.
[45] Art 41 (1) proposed Regulation.

performance of their tasks, support coordination and cooperation amongst such authorities and provide support to victims in connection to the provider's obligations.[46]

The EU Centre will work in close partnership with EUROPOL. After receiving reports from providers and checking them to avoid obviously false positives, reports which are 'not manifestly unfounded' will be forwarded to EUROPOL and to national law enforcement authorities.[47] The EU Centre will be in the same location as EUROPOL (The Hague, Netherlands). EUROPOL and the EU Centre shall provide each other with the fullest possible access to relevant information and information systems and share its administrative functions such as human resources, IT, cybersecurity, and other operational structures.

[46] Art 43 proposed Regulation.
[47] Art 48 (3) proposed Regulation.

4. CONTENTIOUS ISSUES: LEGAL FRAMEWORK, CHALLENGES AND FINDINGS

This section of the report provides a brief presentation of the legal framework of the four thematic areas prioritised for this workshop and summarizes participants' discussions around each of them. It should be noted that most of the discussion referred to the application of the proposed Regulation to open networks. An open network, for the purposes of this report, is a network that does not use any privacy enabling technology (PET) to mask the content of user communications. An example of a PET would be end-to-end encryption.

4.1 PROHIBITION OF GENERAL MONITORING OBLIGATION

Introduction to the legal framework:

The prohibition of a general monitoring obligation is a key element of the existing EU legal framework for platform governance. As the proposed Regulation obliges providers which have received a detection order to actively search for known CSAM, new CSAM and/or solicitation of children, participants discussed whether such an obligation amounts to general monitoring and hence violates existing EU law.

To better understand the background and rationale for the general monitoring prohibition, the workshop supplied an introduction to participants on the evolution of the framework for platform regulation in the EU alongside a brief discussion of the legal and societal challenges.

The European Union's Approach to regulating platforms

The EU's approach to platform governance is based on three principles: first, the country-of-origin principle requires platforms to comply with the laws of the Member States where they are established; second, under certain conditions, the limited liability principle (Articles 12-14, e-Commerce Directive) exempts platforms from any liability arising from the content they host (Article 14, e-Commerce Directive); finally, the prohibition of any general monitoring obligation (Article 15, e-Commerce Directive) ensures the protection of fundamental rights like expression, privacy, and data protection. Article 15 of the e-Commerce Directive is hence a legal provision which aims to protect EU Charter rights.

This 'self-regulatory' or 'hands-off' approach has been linked to both the exponential explosion in user-generated content alongside a litany of systemic risks and harms to the information ecosystem. Alongside increasing concerns about the legal uncertainty of national norms, conflicting court rulings on platform regulation and new societal challenges like disinformation within a human rights framework that protects free expression, the EU has responded with measures that aim to constrain platform power by increasing competition and oversight. It established a harmonized framework, the Digital Services Act 2022, for content management and curation to tackle harmful or illegal content like CSAM more effectively at the supra-national level in a manner that ensures legal clarity and respect for fundamental rights.

Specific versus General Monitoring Obligations

Article 14 of the e-Commerce Directive is a focal point of the European Union's framework for intermediary liability for user-generated content. Article 14 provides safe harbour arrangements

under which platforms cannot be held liable, under certain conditions, for users uploading illegal content. The Article's purpose is to limit intermediary liability to obtain actual knowledge of illegal content or activity. As platforms could be held liable for possession and dissemination of unlawful CSAM uploaded by their users, the e-Commerce Directive's safe harbour provision limits the potential for both criminal and financial consequences for user-generated content; it does not prevent court orders to remove existing (and future) uploads of illegal content.[48]

However, the permissible scope of court orders is limited by a prohibition against **general monitoring**. The latter prevents subjecting intermediaries from a general obligation to monitor the content they host or to **actively find illegal activity.** Recital 47 e-Commerce Directive demonstrates that the prohibition is only applicable to monitoring obligations of a general character; therefore, a monitoring obligation for a specific case is permitted. Recital 48 e-Commerce Directive refers to the applicability of the duty of care to service providers, who can "reasonably" be expected to detect and prevent specific infringements based on national legislation; therefore, the Recital does not impose a duty to remove specific content but refers to the possibility of the imposition of one by Member States.

The European Courts have also been instrumental in determining the nuances of the e-Commerce Directive, especially in defining the difference between an impermissible general monitoring and a permissible specific monitoring obligation. In *Netlog*, the Court of Justice of the European Union (hereafter 'CJEU') considered that mandating a hosting provider to install a filtering system that indiscriminately filters all the content uploaded by each user for an unspecified time was a violation of the prohibition of a general monitoring obligation and hence a violation of the e-Commerce Directive.[49] Yet in *YouTube*[50]*,* Advocate General Saugmandsgaard Øe stated that platforms can be required to identify and take down not only identical infringing content but 'equivalent content' via court-issued injunctions. What is the legal meaning of 'equivalent content'? This amounts to essentially identical material, which might have been slightly altered. In theory, equivalent content can still be detected by certain algorithmic-based technology (including AI) without human intervention. Furthermore, Article 8(3) of the Information Society Directive[51] complements safe harbour provisions under the ECD, enabling copyright owners to obtain injunctions against intermediaries whose services are used. Thus, Article 8(3) can also impose stay-down obligations for known illegal material on intermediaries without violating the prohibition against any general monitoring obligation. Thus, in rulings on intermediary liability cases, the CJEU has focused on striking a "fair balance" between competing interests like the right to intellectual property and the right to privacy; the right to operate a business and the right to data protection; and the right to free expression versus the right to privacy.

The CJEU rulings have thus reduced the former absolutist approach to the prohibition of a general monitoring obligation. In the early cases, the prohibition meant any filtering system would amount to disproportionate interference. In the latter cases, the CJEU has declared that requirements to block

[48] For example, Article 8(3) of the Information Society Directive complements the e-Commerce Directive's safe harbour provisions, enabling copyright owners to obtain injunctions against intermediaries whose services are used by third parties for copyright infringement.
[49] C-360/10, Netlog v Sabam, at para. 26 and 50.
[50]Opinion of Advocate General Saugmandsgaard Øe on Joined Cases C- 682/18 Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH; See also C- 683/18, Elsevier Inc. v Cyando AG.
[51] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

access to "illegal and equivalent content" are not only proportionate but have imposed obligations on platforms to keep illegal content that users wish to upload off their sites. Thus, technology that matches user-generated content against a centralized database of *known* illegal and its equivalent content is a permitted exception to the prohibition of a general monitoring obligation.

According to the CJEU, the defining characteristic of what would amount to prohibited general monitoring is a requirement for online intermediaries to conduct an independent legal assessment of the illegal nature of the content. Service providers cannot be required to prevent uploading and making available to the public content, which, to be found unlawful, would require an independent assessment of the content by the service provider. This position is also replicated in Article 7 of the Digital Services Act: "No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers".

Prohibition of general monitoring obligation in the context of the proposed Regulation

Thus, the court's position can be summarized as follows: there is a prohibition of an obligation to undertake general monitoring of user-generated content. However, platforms can be asked to build systems to block access to *known illegal content* and *equivalent illegal content.* The prohibition of a general monitoring obligation extends to risky or potentially harmful content.

Without safe harbour provisions, every bit of user-generated content would need screening pre-posting. Platforms, web-hosting companies, as well as crucial elements of the internet's infrastructure would be subject to endless claims of wrongdoing for publishing unlawful content. Accordingly, scanning for *new* CSAM and solicitation of children communications could amount to a violation of the prohibition of a general monitoring obligation. A legal obligation requiring platforms to scan user-generated content for *new* CSAM would require both centralized scanning of all existing and uploaded content for the purposes of cross-referencing against the EU Centre's database of indicators.

Discussion:

Most participants agreed that imposing an obligation on platforms to scan for *known* CSAM would not violate the prohibition of a general monitoring obligation because it would amount to specific content deemed *a priori* unlawful by an appropriate administrative or judicial body. Participants shared concerns that imposing obligations on platforms to scan for *new* CSAM and solicitation of children communications could violate the prohibition of a general monitoring obligation. Some participants argued that there is a moral argument for scanning uploads *a priori* posting to intercept illegal material. Other participants voiced concerns about the chilling effects of constant and mass surveillance of all private communications. They also shared concerns that legal obligations that amount to scanning for *new* CSAM, and solicitation of children could amount to a general monitoring obligation on platforms. Some participants argued that looking for *new* CSAM and solicitation of children would not violate the general monitoring obligation. The obligation could be specific (e.g., for certain users where there is suspicion, for instance). Other participants pointed out that this would need a legal basis (i.e., a warrant) and would require targeting a specific user. This would not amount to a violation of the prohibition of general monitoring.

Summary of main discussion points:

- Some participants felt it is not possible for any Member State's national law nor for EU law to impose an obligation to monitor all the content posted by users for potential illegality or for unlawful material.
- Some participants felt it is possible to impose a legal obligation on platforms to scan for and restrict access to specific content or 'equivalent' in nature to something *a priori* illegal or unlawful.
- Some participants felt that scanning all communications for new CSAM and solicitation of children potentially violates the prohibition on a general monitoring obligation.

4.2 PROPORTIONALITY OF THE PROPOSED REGULATION

According to Art 52 (1) EU Charter, any limitation on the exercise of the rights and freedoms recognized by the Charter must be provided for by law and respect the essence of those rights and freedoms. Limitations may be made only if they are proportionate, necessary, and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. This proportionality test is the core of the EU fundamental rights regime and paramount for the establishment of regulatory measures in the EU. In the debate around the proposed Regulation, the term 'proportionality' has largely been used as a political battle cry to either denounce or support the proposed Regulation. However, what has often been missing is a thorough legal engagement with the various aspects of the proportionality test and a sound assessment of the contentious points of the proposed Regulation in this context.

Against this background, the workshop took participants through the various steps involved in the proportionality test as set out in Art 52 (1) EU Charter to better understand the legal parameters involved in measuring the various components of Art 52 (1) EU Charter, to better locate the debate around a specific aspect of the proposed Regulation within the proportionality test and to identify areas for further investigation.

Due to the limited time the workshop participants had available for this exercise, only a few aspects of the proposed Regulation could be debated. Therefore, the below should not be interpreted as a full proportionality assessment of the proposed Regulation, but rather as a snapshot of some contentious points. In particular, the respect for the essence of the rights and the proportionality test in its narrow sense (i.e., the fair balancing of affected rights), was not explicitly debated. This was a deliberate decision by the organizers as it would have been very unlikely that participants would have found any common ground on this. Instead, the organizers wanted to focus participants on other aspects of the proportionality test in Art 52 (1) EU Charter, which have not been the focus of the debate so far but are equally important.

'PROVIDED FOR BY LAW'

Introduction to the legal framework:

The term 'provided for by law' encompasses the requirements of a legal basis, which must be accessible and foreseeable. The EU Commission published the proposed Regulation laying down the

legal framework for the proposed measures, and hence the requirement for the need for a legal basis is fulfilled. Accessibility and foreseeability mean that the proposed Regulation is also accessible to laypersons and that the legal consequence can be sufficiently predicted, i.e., foreseen.

Discussion:

In this context, the participants discussed whether some of the terms used in the proposed Regulation, such as 'reasonable risk mitigation measures' in Art 4 (1)[52], 'appreciable extent' in Art 7 (4) – (6) in the context of the service being used for online CSA, or 'effective' in Art 10 (3) in reference to the deployed technology, are sufficient to meet the criteria of foreseeability, as they arguably enjoy a vast spectrum of interpretation. Even though it was noted that the Commission may issue guidelines on the application of Articles 7-10, it is recommended that open terms especially in the risk assessment and risk mitigation provisions should be clearly defined in the legislation to ensure the goalpost for providers in terms of risk mitigation measures is clearly defined. This will also avoid a different interpretation of these terms on national level, which would defeat the purpose of harmonizing the requirements imposed on providers of relevant online services in the digital single market.

'MEET OBJECTIVES OF GENERAL INTEREST'

Introduction to the legal framework:

The proposed Regulation states that it pursues an objective of general interest, which is the harmonization of rules that apply to prevent and combat child sexual abuse. It aims to protect the rights of children, namely their fundamental rights to human dignity and the integrity of the person, the prohibition of inhuman or degrading treatment, as well as the rights of the child.[53]

Discussion:

Participants agreed that the proposed Regulation indeed pursues an objective of general interest.

'NECESSARY'

According to Art 52 (1) EU Charter, limitations of fundamental rights need to be necessary. This means that the legislation needs to be effective, as measured by a fact-based assessment proving that the envisaged measures achieve the pursued objective and need to be the least intrusive for affected fundamental rights compared to other available options.[54]

Participants discussed various aspects in the context of the necessity criteria, as shown below:

PREVIOUS INSTANCES OF ONLINE CSA AS CRITERIA FOR THE RISK ASSESSMENT IN ART 3 (1)

Introduction to the legal framework:

[52] All articles cited in this report are those of the proposed Regulation, unless described otherwise.
[53] See proposed Regulation, p. 12.
[54] EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 2017, p. 5.

As set out in Art 3 (1), providers of hosting services and providers of interpersonal communications services must conduct a risk assessment to assess the risk of their service(s) being used for the purpose of online CSA.

One of the criteria to assess the risk associated with a service is whether the provider encountered any previously identified instances of the use of its services for the purpose of online CSA. In this context, participants discussed whether this criterion is indeed effective. As the Interim Regulation ceases with the entry into force of the proposed Regulation, providers cannot rely on the Interim Regulation anymore to voluntarily scan for online CSA on their services (see section 4.4 of this paper discussing the possibility of continued voluntary detection). Therefore, providers will generally have to rely on user reports and reports from trusted flaggers to assess the risk of online CSA on their platforms. In this context, the question arises how the Coordinating Authority will verify whether the data provided by the provider on previous instances of online CSA are indeed factual. The Coordinating Authority might be able to request reports from trusted flaggers; however, this is not mentioned in the Regulation as a possible verification mechanism. As for user reports, it is not clear how the Coordinating Authority intends to verify the reports by providers. This carries the risk that providers will incorrectly report the instances of online CSA reported to them, without the Coordinating Authority being able to verify the provided figures. This is a significant issue considering that previous instances of online CSA on a service are not the only, but certainly a key criterion in the risk assessment to be conducted under Art 3.

Discussion:

Participants, therefore, agreed that the proposed Regulation should include a verification mechanism to assess the risk on services and platforms independently.

TIMELINESS OF RESPONSE: FROM IDENTIFICATION OF POTENTIAL ONLINE CSA CASES TO VICTIM IDENTIFICATION AND SUPPORT

The participants discussed the effectiveness of the proposed Regulation in the context of the time between flagging potential online CSA and the initiation of investigations that could lead to a child being safeguarded. Additional concerns were raised about the time, the necessity of identifying the children depicted in CSAM, and the potential of the proposed Regulation, when implemented, to disrupt the solicitation of children.

Introduction to the legal framework:

It is important to differentiate between known CSAM, new CSAM and solicitation of children. Known CSAM will be identified by comparing a file against a CSAM database; understandably, it is likely that law enforcement has already conducted some degree of analysis to determine the illegality of the content. In contrast, cases of potential new CSAM and solicitation of children will most likely reveal recent or ongoing abuse, requiring a timely response from law enforcement to potentially initiate investigation and identification procedures.

When following the 'chain of command' in the proposed Regulation, it is the role of the provider to make a first assessment of the potential online CSA once detected by the technology solutions. Even though the technology solutions applied by providers will flag potential online CSA, human moderation will play a key role to assess whether the flagged item indeed constitutes online CSA,

especially when it comes to potential new CSAM and potential solicitation of children.[55] After the assessment by the provider, the provider is obliged to report the potential online CSA to the EU Centre (Art 12 (1)). The EU Centre shall 'expeditiously' assess, and process reports submitted by providers to determine whether the reports are 'manifestly unfounded,' (Art 48 (1)). Where the EU Centre finds that the report is not manifestly unfounded, it shall forward the report to EUROPOL and to the competent law enforcement authority likely to have jurisdiction to investigate the case. After receiving the report, law enforcement starts its investigation, which hopefully leads to the rescue of the child and subsequently to the prosecution and conviction of the perpetrator. However, it is not clear how long the EU Commission estimates this process will take. It is noticeable that the proposed Regulation does not set time limits for the assessment conducted by the provider or by the EU Centre.[56]

Discussion:

Participants agreed that the lack of clear timeframes concerning the identification of CSA cases needs to be urgently addressed in the proposed Regulation, considering that especially solicitation cases can escalate within a few hours, potentially leading to serious harm to an affected child.

Considering the vast number of potential cases to be assessed by providers as the first entry point for potential online CSA, participants debated whether the proposed Regulation should include a prioritisation system, which assists providers in flagging when a child is in acute danger, so the EU Centre and law enforcement could prioritize these cases. While some participants would find such prioritisation useful, other participants questioned whether this would be implementable in practice. Firstly, the question arises about which criteria providers should use in developing a prioritised flagging system. Secondly, whether providers could identify prioritized cases solely based on the material or the communication they are assessing. Participants expressed that to identify cases of acute danger, additional evidence would be required, which is not necessarily accessible to providers and that they would neither have the legal basis nor the capacity to collect and analyze. The investigation of such circumstantial, corroborative evidence is the mandate of law enforcement. It is only possible once cases have been referred to national law enforcement or to EUROPOL by the EU Centre.

In addition to the lack of a clear timeline for the assessment of potential online CSA cases by the provider and the EU Centre, another concern raised by participants in terms of timeliness of response occurs in the context of national law enforcement capacity. In the impact assessment, the Commission points out that 'immediate long-term assistance [for victims] remains limited'.[57] It further states that 'significant investment of resources [are] required for law enforcement to deal effectively with the volume of reports these authorities receive'.[58] This raises the question of how both victim support

[55] Hereby, it is worthwhile to note that it is not clear which standard providers have to use when assessing flagged material. It is assumed that the definitions contained in Art 2 apply; however, this should be clearly stated in the proposed Regulation.

[56] It must be noted that the proposed Regulation sets a 24h timeframe for providers to execute removal orders, see Art 14 (2) proposed Regulation.

[57] EU Commission, *Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, SWD(2022), 209 final*, p. 23.

[58] EU Commission, *Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, SWD(2022), 209 final*, p. 33.

services and law enforcement will cope with a considerable increase in workload if the proposed Regulation enters into force in its current form.

Some participants proposed that the impact assessment should assess the timeliness of response in law enforcement and social welfare capacity at the national level, especially for cases of new CSAM and solicitation of children. Such a capacity assessment is key to understanding whether the proposed Regulation is effective in identifying and supporting child victims of online CSA – considering that these are not the sole objectives of the proposed Regulation: removing CSAM and preventing its further distribution is also contributing to ending CSA.

EFFECTIVENESS OF PROPOSED TECHNOLOGY SOLUTIONS

Introduction to the legal framework:

Art 10 (1) states that providers shall execute detection orders by installing and operating technologies to detect online CSA, using the indicators provided for by the EU Centre. Providers can choose to develop their own technology or use technology made available by the EU Centre if the technology meets the following requirements:

a. Effective in detecting the dissemination of online CSA;
b. Not able to extract any other information than the information strictly necessary to detect online CSA;
c. Technology is in accordance with the state of the art in the industry and the least intrusive; and
d. Technologies are sufficiently dependable - in that they limit to the maximum extent possible the rate of false positives.[59]

Discussion:

Participants in the workshop discussed whether the above criteria are sufficient to determine when technology is ready for deployment. Some participants raised concerns regarding the proposed technologies cited in the impact assessment as being state-of-the-art and questioned whether these are indeed ready for use. Considering that the Commission cited the Microsoft Artemis project as suitable technology, with Microsoft asking the Commission in turn to stop citing this technology in the context of the proposed Regulation as suitable measures[60], shows that there is no clarity when exactly the threshold of Art 10 (3) will be reached. Further, participants questioned whether the process for assessing the suitability of proposed technology for deployment by providers by the EU Centre is sufficiently transparent and regulated.

Participants agreed that the criteria in Art 10 (3) need to be further defined and need to be clearly measurable. This would illuminate the *de facto* impact of such technologies on users' fundamental rights to privacy and data protection. Clear thresholds and criteria would also assist in making the proposed Regulation technology neutral while avoiding technologies that are not ready yet for

[59] Art 10 (3) proposed Regulation.
[60] Microsoft position paper on the proposal for a Regulation laying down rules to prevent and combat child sexual abuse, available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online/F3338552_en.

deployment being recommended by the EU Centre. Regarding the assessment process set out in Art 50, participants proposed that the effectiveness and *modus operandi* of the technology must be evaluated by an independent body. The EU Centre, and with it the Technology Committee mandated to advise the EU Centre (see Art 66), should not simply rely on data provided by the company developing the technology (as has been done in the proposed Regulation and the impact assessment), to ensure that the provided evidence is factual.

In the context of solicitation of children, some participants further enquired whether the sole deployment of such technology is effective in leading to more investigations and prosecutions. The question was raised about how solicitation of children cases are currently investigated and prosecuted in EU Member States, as this is important evidence to understand whether the referral of potentially illegal communication to law enforcement leads to more victim rescue, prosecutions, and convictions. As an example, it was discussed whether chat logs would amount to probable cause and hence be sufficient to justify the issuing of a search warrant to collect corroborating evidence. In this context, participants agreed that the Commission should include this information in the impact assessment to better understand how the proposed Regulation will assist in achieving the pursued objective.

PROPORTIONALITY AND DETECTION ORDERS:

Introduction to the legal framework:

When discussing the proportionality of the proposed Regulation, it must be noted that the ultimate decision of whether a detection order is issued will not be decided at the EU, but at the EU Member State level. As set out in Art 7 (1), Coordinating Authorities can request either a judicial or an independent administrative authority to issue a detection order. When deciding whether such a detection order should be issued, the judicial authority or independent administrative body must verify that there is evidence of significant risk of the service being used for online CSA (see section 3.1 for the detection order requirements) and that the reasons for issuing the detection outweigh negative consequences for the rights and legitimate interests of all parties affected. The latter resembles the proportionality requirement as set out in Art 52 (1) as part of the proportionality test.

Discussion:

Participants raised several questions regarding the design of the detection order issuing process. First, considering the potential intrusiveness of such an order, particularly if issued for the detection of new CSAM or solicitation of children, participants deliberated whether an independent administrative body should be authorised to make this decision. As an independent administrative body forms part of the executive, some participants argued that only a judicial body should be authorized to issue detection orders under the proposed Regulation to better protect affected fundamental rights.

Further, some participants raised concerns that the ultimate decision for proportionality is pushed to national courts, even though the legislator itself should take this decision. While the reason for pushing the final decision-making power to the national level presumably lies in the principle of subsidiarity, it raises the question of whether the process of issuing detection orders as currently set out in the proposed Regulation will be effective and applied harmoniously across the EU. While the Commission may publish guidelines on the issuance of detection order, it is likely that national courts undertake the proportionality test in vastly diverse ways, creating diverging standards and

assessments across Member States. Accordingly, there is a risk that similar services with comparable risk assessments will face detection orders assessed and issued according to different standards. If this scenario becomes reality, the proposed Regulation will contravene the purpose of Art 114 of the Treaty on the Functioning of the European Union (hereafter 'TFEU') in terms of the functioning of the internal market. This is highly problematic as the Commission issued the proposed Regulation in the first place by arguing that Art 114 TFEU is the applicable legal foundation. If the proposed Regulation does not *de facto* contribute to the harmonization of the requirements imposed on providers of online services in the Digital Market, it is questionable whether the Commission even has the legal authority for the proposed Regulation.

Summary of main discussion points:

- Open terms such as 'appreciable extent' should be clearly defined in the proposed Regulation to ensure accessibility and foreseeability for affected providers.
- The proposed Regulation should include a verification mechanism to independently assess the risk identified by providers on services and platforms in the risk assessment stage.
- The proposed Regulation should set clear timeframes in which providers and the EU Centre assess and transfer potential online CSA reports to ensure cases are dealt with swiftly.
- To be in a better position to understand whether the proposed Regulation is effective in identifying and supporting child victims of online CSA, all Impact Assessment reports should include a scenario which assesses the timeliness of response, especially for cases of new CSAM and solicitation of children.
- The proposed Regulation should clearly define criteria for the suitability of technologies described in Art 10 (3), including procedural safeguard, transparency, and accountability standards.
- The Impact Assessment report should include insights on how solicitation of children cases are currently investigated and prosecuted in EU Member States as this is important evidence to understand whether the referral of potentially illegal communication to law enforcement would indeed lead to more victim rescue, prosecutions, and convictions.
- Granting the decision of detection orders to national authorities carries the risk that the proportionality test will be applied differently in each national context, creating diverging standards and assessments across Member States.

4.3 CONSENSUAL ONLINE SEXUAL EXPLORATION BETWEEN ADOLESCENTS

Introduction to the legal framework:

One of the main discussion points of the workshop was how the proposed Regulation deals with consensual online sexual exploration between adolescents via text, photo, video, or other content. Sexuality, identity, intimacy, and interpersonal connection are matters of interest to adolescents in

their journey of identity exploration and construction.[61] While these areas have been traditionally explored and constructed in offline interactions, the online environment is an increasingly important realm for such activities.[62] Similar to in-person sexual exploration, online sexual exploration comes with potential risks for adolescents. These risks can result in harm if not identified and managed properly.

Visual assessment of content alone makes it challenging to determine whether a sexual image/video involving a person appearing to be an adolescent depicts consensual sexual exploration or the sexual abuse or exploitation of a child. Without additional evidence and context, the circumstances under which the material was produced cannot be taken into consideration, which can lead to the consensual online sexual exploration between adolescents being categorized as online CSA offences.[63] However, both the United Nations Committee on the Rights of the Child (hereafter 'CRC Committee') and the Council of Europe advocate for the decriminalization of consensual sexual exploration, acknowledging that such conduct is increasingly considered normal by adolescents[64] and citing specific circumstances under which such content should be decriminalized, e.g., if the children produce/possess/disseminate such content voluntarily and consensually for their private use.[65] The Council of Europe suggests that this should, under very narrow circumstances, equally apply to consensual online sexual exploration between an adolescent and an adult of a similar age and maturity[66], for example, a 17-year-old and an 18-year-old.

Against this background, the question arises of how the proposed Regulation will deal with digital content produced through consensual online sexual exploration amongst adolescents. Suppose a detection order is issued for the identification of new CSAM and/or the detection of solicitation of children. In that case, such a detection order applies, due to the lack of a limitation of its scope in Art 7, also to conversations between two children, i.e., persons below the age of 18 years. It is crucial to point out that the technology deployed to detect new CSAM or solicitation of children will not be able to differentiate between consensual and non-consensual sexual conversations or sexual image sharing between adolescents in a private conversation. The technology is indicator-based and will hence flag any form of child nudity/sexual activity with a child/sexual conversation with a child, regardless of the

[61] Sabine K. Witting, *Child sexual abuse in the digital era: Rethinking legal frameworks and transnational law enforcement collaboration*, Leiden 2020

[62] David Smahel/Kaveri Subrahmanyam, *Adolescent Sexuality on the Internet: A Developmental Perspective* in: Fabian M. Saleh/Albert J. Grudzinskas/Abigail M. Judge, 'Adolescent sexual behavior in the digital era,' Oxford 2014, p. 62.

[63] Council of Europe, Lanzarote Committee report on *The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs) - Addressing the challenges raised by child self-generated sexual images and/or video (Implementation Report),* Strasbourg 10 March 2022; Witting, *Child sexual abuse in the digital era – Rethinking legal frameworks and transnational law enforcement collaboration,* p. 41.

[64] CRC Committee, *Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography*, CRC/C/156, para. 42.

[65] Council of Europe, Lanzarote Committee *Opinion on child sexually suggestive or explicit images and/or videos generated, shared, and received by children*, Strasbourg 2019 and Lanzarote Committee report *The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs) - Addressing the challenges raised by child self-generated sexual images and/or video (Implementation Report)*, Strasbourg 10 March 2022.

[66] Council of Europe, Lanzarote Committee report on *The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs) - Addressing the challenges raised by child self-generated sexual images and/or video (Implementation Report)*, Strasbourg 10 March 2022.

context or the age of the other user involved. This means that it is likely that providers who are forced to deploy such technology through a detection order will flag all consensual sexual exploration amongst adolescents as potential online CSA and refer it to the EU Centre.

Discussion:

Against this background, participants discussed the impact of this issue on children's right to privacy and personal data protection. Participants suggested that the EU Centre as the 'gatekeeper' between providers and law enforcement/EUROPOL should play a key role in identifying consensual content and subsequently not refer such content to law enforcement/EUROPOL to avoid prosecution of such cases on the EU Member State level. However, other participants pointed out that the EU Centre is not in a legal position to exclude such material from the scope of the definition of online CSA. As set out in Article 2, the EU Centre applies the legal definitions of the CSA Directive. This Directive '*does not govern Member States' policies with regard to consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development*' (Recital 20 CSA Directive). Art 8 (3) of the CSA Directive states that '*it shall be within the discretion of Member States to decide whether Article 5(2) and (6) apply to the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse*'. This means that the CSA Directive considers consensual online sexual exploration amongst adolescents as a criminal offence *unless* the EU Member States decriminalize it.

Considering that the CSA Directive is currently under review[67], participants made a compelling case for including an exemption clause for online consensual sexual exploration between adolescents in the revised CSA Directive to ensure these cases are not referred to law enforcement/INTERPOL for further investigation. However, even if such an amendment becomes a reality, it is unlikely that the EU Centre will practically be able to differentiate consensual from non-consensual content as this requires more context information and further details. Such circumstantial evidence will usually only be collected by law enforcement on the national level and in many cases, will not be obtained until the people depicted in the content are identified.

Accordingly, most consensual online sexual exploration cases will end up with national law enforcement/EUROPOL for investigation. Participants hence discussed the consequence for affected adolescents. EU Member States take a vastly different approach to the issue. Only a few EU Member States (namely Austria, Cyprus, Germany, Finland, and Croatia) have chosen to apply Art 8 (3) CSA Directive and subsequently decriminalized certain consensual online sexual activities amongst adolescents.[68] However, further research shows that some EU Member States decided not to

[67] See here: https://ec.europa.eu/info/law/better-Regulation/have-your-say/initiatives/13073-Combating-child-sexual-abuse-review-of-EU-rules_en

[68] The Lanzarote Committee found that the EU Member States that are also Parties to the Lanzarote Convention that chose to apply the exemption of Article 20(3) of the Lanzarote Convention did not systematically also chose to apply Article 8(3), see Council of Europe, Lanzarote Committee report on *The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs) - Addressing the challenges raised by child self-generated sexual images and/or video (Implementation Report)*, Strasbourg 10 March 2022.

prosecute such activities. At the same time, many EU Member States either openly criminalize such consensual online exploration or do not have a clear legal position on it, risking children's prosecution for such behaviour.[69] Participants agreed that a more profound understanding of how EU Member States deal with such cases is required to assess the impact on children's rights. Participants are seeking more clarity on how the Commission aims to respond to the consensual online sexual exploration of adolescents in the context of the proposed Regulation.

Regardless of how the EU Centre or national law enforcement will eventually deal with such material, some participants raised that the moderation and flagging of consensually produced and shared content in and of itself might constitute a child rights violation. It was argued that the use of digital technologies, which leads to the exposure of the most intimate and private part of children's lives, their sexuality and sexual expression, might be a violation of their right to privacy as protected under Art 7 EU Charter. Others argued that children also commit child sexual abuse online. Hence, the legislation might fail children abused by peers if any content produced and shared amongst children were to be excluded from the scope of the proposed Regulation by default. Participants agreed that more understanding is required of how platforms would moderate and respond to such content, who the content moderators are, and how they are trained.

Lastly, participants agreed that this is an area of the proposed Regulation where consultations with a diverse group of children and adolescents would be most beneficial to ensure that their views are at the centre of the formulation of such EU legislation.

Summary of main discussion points:

- The EU Centre, as the 'gatekeeper' between providers and law enforcement/EUROPOL, should play a key role in identifying consensual content and subsequently not refer it to law enforcement/EUROPOL to avoid investigation/prosecution of such cases on the EU member state level.
- As the applicable legal standard for defining the scope of the proposed Regulation, the CSA Directive should include an exemption clause for online consensual sexual exploration between adolescents under specific circumstances, as advocated for by the CRC Committee and the Council of Europe Lanzarote Committee.
- As the EU Centre might not be able to differentiate consensual from non-consensual content as this requires more context information and circumstantial evidence, the Impact Assessment of the proposed Regulation should provide insights into how cases of consensual content are dealt with by national law enforcement to gain a better understanding of the child rights impact.
- Moderation and flagging of consensually produced and shared sexual content by adolescents in and of itself might violate children's right to privacy as protected under Art 7 EU Charter as it exposes the most intimate and private sphere of adolescents' lives (their sexuality and sexual expression).

[69] Argyro Chatzinikolaou/Eva Lievens, *A legal perspective on trust, control, and privacy in the context of sexting among children in Europe*, Journal of Children and Media, 14:1, 38-55.

- Consultation with a diverse group of children and adolescents would be beneficial to ensure that their views are at the centre of formulating a policy decision and subsequent Regulation.

4.4 CONTINUED VOLUNTARY DETECTION OF ONLINE CSA

Introduction to the legal framework:

The fragmented nature of the e-Commerce Directive permitted platforms to develop their own procedures for content moderation in a manner that aligned best with their own business models. Most mainstream platforms have a vested interest in self-regulating and policing content for CSAM - the proliferation of this type of content could seriously harm their business models and support among their shareholders. Nevertheless, many platforms remain not regulating the circulation of CSAM on their services and do not take any other action to prevent and respond to online CSA. Self-regulation is also blamed for platforms favouring a quantitative analysis of the virality of individual content rather than any qualitative analysis of the value (and risk) associated with that content. As a result, platforms have lacked any real motivation to moderate "harmful" but lawful content. Innovative thinking is needed on how to motivate platforms to voluntarily detect unlawful content as well as content that might be harmful but does not quite hit the threshold of unlawful.

A point often raised by child rights organizations is the need for a legal basis to allow providers to continue the voluntary detection of online CSA on their products and services, even after the proposed Regulation enters into force and even if they have not received a detection order.[70]

To provide some background: since the entry into application of the 2018 European Electronic Communications Code Directive[71] on 21 December 2020, the e-Privacy Directive also covers number-independent inter-personal communication services (hereafter 'NIICS') such as messaging services and email. Thus, the ePrivacy Directive prevented such NIICS from continuing their voluntary use of specific technologies to detect online CSA without authorization by national or EU legislation. To avoid such voluntary practices coming to a complete halt in the EU following 21 December 2020, the Interim Regulation entered into force on 2 August 2021 enabling NIICS to continue the voluntary use of technologies for the processing of personal data and other data to the extent necessary to detect, report, and remove child sexual abuse online. However, this Interim Regulation ceases to apply three years after its entry into force (3 August 2024) and will be replaced by the proposed Regulation which does not include any legal provisions to continue the voluntary detection regime provided for in the Interim Regulation. The Commission makes it clear in its proposed Regulation that this was a deliberate decision:

> '*The Processing of users' personal data for the purposes of detecting, reporting, and removing online child sexual abuse has a significant impact on users' rights and can be justified only in*

[70] In this context, the recommendations from the Council of Europe's Independent Experts' report should be considered, see Council of Europe, *Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse*, June 2021.

[71] Directive 2018/1972 of the European Parliament and of the Council on 11 December 2018 establishing the European Electronic Communications Code (Recast) (OJ L 321, 17.12.2018).

view of the importance of preventing and combating online child sexual abuse. As a result, the decision of whether to engage in these activities in principle cannot be left to the providers; it rather pertains to the legislator'[72].

This shows that the Commission places the responsibility for deciding on the use of detection technology with the legislator, considering the significant impact on users' rights.

Discussion:

Some participants argued that the continuation of some sort of voluntary detection regime is paramount to avoid detection gaps and allow providers to proactively detect online CSA on their products and services, even if they have not received a detection order which legally obliges them to do so. Other participants raised that the lack of a legal foundation for the processing of personal data has been a main point of critique already during the development of the Interim Regulation.[73] According to Art 6 (1) GDPR, processing personal data is only lawful if one of the grounds set forth in Art 6 (1) GDPR applies. As the Interim Regulation does not legally oblige but solely gives NIICS the opportunity to continue voluntary detection of online CSA, it has been argued that the processing of personal data cannot be based on Art 6 (1) (c) GDPR ('processing is necessary for the compliance with a legal obligation'). The Commission seems to agree with this position, stating in the Impact Assessment report that the 'Interim Regulation does not establish a legal basis for any processing of personal data'.[74] Further, the Impact Assessment report notes that some providers evoked other legal bases in the GDPR for the processing of personal data.[75] While the report does not give explicit examples of which these bases are, participants assumed that the processing is either based on the consent of the data subject (Art 6 (1) (a) GDPR) or the legitimate interest of the controller (Art 6 (1) (f) GDPR). However, the legal uncertainty around the legal basis for the processing of personal data under the GDPR seems to have deterred some providers of deploying voluntary detection technology in the past, according to the Impact Assessment report.[76]

If the continued voluntary detection were not based on the Interim Regulation, participants discussed under which circumstances providers could continue such a practice. A possible avenue for continued voluntary detection is the consent of users for the deployment of such detection measures (as this would provide for a legal basis under both the GDPR and the e-Privacy Directive). However, other participants noted that consent from users needs to be *informed* to be valid, and that this might not be the case if such measures were 'hidden' in terms and conditions, especially in the case of child users.

[72] Proposed Regulation, p. 14.
[73] EDPS, *Opinion 7/2020 on the Proposal for temporary derogations from Directive 2022/58/EC for the purpose of combatting child sexual abuse online*, November 2020.
[74] EU Commission, *Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, SWD(2022), 209 final*, p. 10.
[75] EU Commission, *Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, SWD(2022), 209 final*, p. 35.
[76] EU Commission, *Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, SWD(2022), 209 final*, p. 35.

Summary of main discussion points:

- Some participants raised concerns that the Interim Regulation ceases to apply three years after its entry into force (on 3 August 2024) and will be replaced by the proposed Regulation which does not include any legal provisions to continue the voluntary detection regime provided for in the Interim Regulation.
- Other participants raised that the legal uncertainty around the legal basis for the processing of personal data under the GDPR seems to have deterred some providers of deploying voluntary detection technology in the past. As the Impact Assessment report states that the Interim Regulation does not establish a legal basis for any processing of personal data under the GDPR, they did not see a legal basis for any continued processing of personal data as part of the voluntary detection regime.
- Participants acknowledged that continued voluntary detection as it is currently established by the Interim Regulation is less likely.
- Participants explored other possible avenues for continued voluntary detection, such as the consent of users for the deployment of such detection measures; however, it must be noted that such consent needs to be *informed* to be valid, and that this might not be the case if such measures were simply 'hidden' in terms and conditions.

5. AREAS FOR FURTHER INTERROGATION AND IDENTIFYING COMMON GROUND

In this section, we will shift the focus towards areas for further interrogation and identifying common ground. Apart from the pre-selected topics discussed by participants under section 4, participants identified areas of the proposed Regulation which require further discussion and clarity to assess the impact of the proposed Regulation. Further, participants worked in groups to identify common ground regarding the proposed Regulation, i.e., parts of the proposed Regulation all participants across various fields do indeed support or where they agree that additional regulatory measures are required. Even though this was a challenging task considering the overall strongly differing opinions on the proposed Regulation, participants succeeded to find some common ground.

5.1 AREAS FOR FURTHER INTERROGATION

ERRORS IN DRAFTING AND SIMPLIFICATION OF PROPOSED PATHWAYS

Participants identified several problematic incidents with the drafting of the proposed Regulation. Examples were provided during the discussion of cross-references that went nowhere, terminology deployed without any clear context or meaning. Other criticisms of the proposed Regulation levied included the inclusion of ambiguities created using double negatives in the drafting of the text (e.g., “not manifestly unfounded”). The proposed Regulation requires more explicit language with closer attention paid to the deployment of systematic referencing to other pieces of legislation. This will considerably improve the accessibility and readability of the proposed Regulation.

More specifically, participants called for a road map of the pathway taken after content is flagged. The pathway taken post-flagging referral is of utmost importance to a) determine the relevant actors involved in any potential infringement of privacy and b) identify any possible flashpoints during the actual content moderation.

INDICATORS, E2EE, AND POTENTIAL PROFILING

During the discussion of the points in section 4, participants had usually not specified whether their comments were limited to open-ended platforms or extend to end-to-end encrypted environments. When specifically mentioned, there were concerns raised about the implications of the proposed Regulation for platforms that use end-to-end encryption (hereafter ‘E2EE’) to ensure some level of confidentiality in communications. The obligation to ensure content was scanned for both known and unknown CSAM and solicitation of children would require platforms to integrate ‘back doors’ into their system architecture, which allow for exceptional access to communication data for law enforcement, or enable client-side scanning, i.e., scanning any outgoing communication directly on the personal device. The introduction of such measures would facilitate scanning and filtering for online CSA even in an encrypted environment. The imposition of a legal rule that requires *de facto* back-door access or client-side scanning to private, encrypted communications has serious implications with respect to the fundamental right to privacy. It would elevate private actors to an entirely new level of gatekeepers working at the behest of state actors. Some participants expressed concern at a lack of understanding of E2EE by the EU Commission and how (and whether) the technology works in such environments. One participant went further, suggesting that the proposed Regulation would effectively require the end of decentralized E2EE.

Participants also expressed concern about the lack of clarity about what could amount to an 'indicator.' There were concerns about what kind of processing and profiling would need to take place for the technology to be sufficient and efficient in its means to achieve its ends. The proposed Regulation states that information used to create an indicator is collected by Coordinating Authorities, courts or other 'independent authorities' [77](hereafter 'IAs'). Still, there is little to no clarity of who the IAs are and how they forward these instructions to the EU Centre. There is also little to no guidance in the proposed Regulation about how the indicators work and what the threshold is for successful deployment. Further concern was posited about the training data used to help the machine model 'learn' what an indicator might look like. A number of participants expressed concern at how there was a lack of transparency in the mechanisms behind the technology used and how it would interact with other legal regimes; for example, would there be a legal basis to object to an automated decision about the flagging of communications for further examination.[78] As there is a legal obligation to place a 'human in the loop' when making decisions that amount to either 'legal effect' or 'similarly significant effect'[79], additional questions were raised about human access to private communications and their ability to determine the context of private communications accurately.

AGE VERIFICATION/AGE ASSESSMENT

In the context of solicitation of children, participants discussed whether the introduction of age verification and age assessments as currently foreseen in the proposed Regulation are effective to protect children from online sexual abuse. The proposed Regulation requires providers of interpersonal communication services, which identified a risk of solicitation of children in their risk assessment, to deploy 'necessary age verification and age assessment measures to reliably identify child users on their services' as a risk mitigation measure[80]. Further, the proposed Regulation states that detection orders in the context of the solicitation of children are limited to interpersonal communications where one of the users is a child user.[81] This limitation is understandable, as otherwise, sexual conversations between adults might falsely be flagged as a potential solicitation of children. The classifiers used to detect solicitation of children cannot necessarily derive from the conversation alone that the parties involved are indeed adults. It is assumed that this limitation was introduced to avoid the straightforward disproportionality of the proposed Regulation.

However, by limiting detection orders to conversations whereby at least one user is a child (see Art 7 (7)), the proposed Regulation introduces age verification and/or age assessment as a mandatory standard for providers. A provider that scans all communication for potential solicitation of children, regardless of the age of the communicating parties, would act without legal basis under the GDPR and the e-Privacy Directive. The proposed Regulation only authorizes such measures for communications in which at least one user is a child. To avoid liability, the Regulation forces providers to introduce age verification and/or age assessment measures before implementing any detection orders.

Some participants raised concerns that age verification/age assessment was introduced by the proposed Regulation through the 'back door' without any consideration of children's privacy and

[77] See Article 44 (1) proposed Regulation.
[78] See Article 22 GDPR.
[79] See Article 22 GDPR.
[80] Art 4 (3) proposed Regulation.
[81] Art 7 (7) proposed Regulation.

personal data. They stressed that age verification does not only raise ethical and legal questions about the fundamental rights of children using their service, but also of adults and young people who would equally have to undertake this verification process.

Most importantly, the proposed Regulation does not set any legal standard on *how* to conduct age verification/age assessments, including a lack of regulation of private providers licensing this technology to platforms for the purposes of verifying users' ages. Even though the EU Commission in its Better Internet for Kids (BIK+) Strategy (2022) aims to set certain standards for age verification[82], it is not clear whether this would include legally binding standards. In practice, current age verification and age assessment measures greatly differ in their effectiveness and intrusiveness regarding children's right to privacy and personal data protection. For instance, having to subject faces to biometric testing to prove age to converse with other users raises additional questions about lawfulness and proportionality and the potential infringements of other users' fundamental rights. Biometrics and facial recognition technologies are widely considered among the most invasive forms of data processing, with some countries going as far as issuing bans on their deployment.

The mandatory introduction of measures without setting any procedural and substantive safeguards of how the requirement should be implemented can open the door for subsequent violations of fundamental rights. The mandatory deployment of age verification systems is fraught with risk. Participants called for a strong impact assessment to determine what safeguards are needed leaning on previous legislative experiences such as the 2018 Audio Visual Media Services Directive[83] and children's data protection law to justify the inclusion of additional invasive technology to achieve compliance with another legal obligation.

Considering the negative consequences associated with a conversation flagged as potential solicitation of children, it makes a difference whether a person is 18 years or 17 years old - only conversations between an adult and a child should be flagged. Suppose age verification, age assessment or other age determination measures are introduced as legal requirements. In that case, the Commission must clearly state the necessary procedural and substantive safeguards for the effectiveness of such measures and procedural and substantive protection for children's and adult users' privacy and personal data.

RELATIONSHIP BETWEEN EU CENTRE AND EUROPOL

To support the implementation of the proposed Regulation, the EU Centre will be established as an independent body of the Union with legal personality.[84] The EU Centre will facilitate the risk assessment, detection, reporting and removing processes. A central task is hereby the creation, maintenance, and operation of databases of indicators of online CSA which providers use to comply with the detection orders. The EU Centre will also make technologies available to providers for the

[82] EU Commission, A Digital Decade for children and youth: the new European strategy for a better internet fir kids (BIK+), COM(2022) 212, 11.5.2022.
[83] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.
[84] Art 41 (1) proposed Regulation.

execution of detection orders. Further, the EU Centre will assist competent national authorities in the performance of their tasks, support coordination and cooperation amongst such authorities, and provide support to victims in connection to the provider's obligations.[85]

The EU Centre will work in close partnership with EUROPOL. After receiving reports from providers and checking them to avoid obviously false positives, reports which are 'not manifestly unfounded' will be forwarded to EUROPOL and to national law enforcement authorities.[86] The EU Centre will be in the same location as EUROPOL (The Hague, Netherlands). EUROPOL and the EU Centre shall provide each other with the fullest possible access to relevant information and information system and share its administrative functions such as human resources, IT, cybersecurity, and other operational structures.[87]

Some participants expressed the need for a better understanding of how such independence were to be enforced if the EU Centre and EUROPOL share certain administrative functions. Others called for clear independence, both in law and in practice, between the EU Centre and EUROPOL. They suggested there need to be strict conditions alongside auditing and oversight of any data/information sharing between the EU Centre and EUROPOL. Further, participants requested a clearer overview of the powers and duties of the EU Centre, EUROPOL, and national law enforcement agencies, respectively. It is not obvious what the referral pathway for potential online CSA cases is between the three entities. It is certainly not clear what minimum safeguards are required for each entity when handling a referral of a private communication that is not clearly illegal ('manifestly unfounded'). Taken together, a broad range of indicators could result in law enforcement accessing and reviewing a substantial number of private communications where there was no unlawfulness.

ROLE OF SELF-REPORTING, TRUSTED FLAGGERS, AND HOTLINES

Participants offered numerous examples of how the technical approaches suggested under the proposed Regulation could be improved by additional safeguards. For example, almost all participants agreed that there should be a legal mandate and standards for providers to improve the ease with which a child can report illegal and unwanted behaviour alongside obligations, in certain contexts, for user confidentiality and access to mental health services and tailored support for victims. Several participants suggested that increased legal status should be provided for dedicated and anonymous hotlines (as part of the ecosystem) alongside guaranteed funding for reporting and support services.

One participant argued that victims should also be part of the reporting mechanism – including suggesting appropriate warnings or sanctions relative to the nature of the offence.

Participants also expressed concern at the health and safety of the humans in the middle of any moderation and examination of online CSA. Although users can report content and problematic communication, human review will still be an important part of identifying potentially illegal material and behaviour. Requiring humans to make the 'final call' on potentially millions of images, videos and conversations will come with a human cost. Some participants, therefore, called for the proposed Regulation to be extended to cover mental health support for content moderators.

[85] Art 43 proposed Regulation.
[86] Art 48 (3) proposed Regulation.
[87] Art 53 (2) proposed Regulation.

ACTIVE PARTICIPATION OF CHILDREN IN THE FORMULATION OF PROPOSED REGULATION

Whenever the EU is developing laws or policies that have a significant impact on the fundamental rights of children, children should be consulted from the get-go. Development and implementation of a policy that affects children should always be evidence-based and child-centred. This derives directly from Art 24 (1) EU Charter which states that children 'may express their views freely. Such views shall be taken into consideration in matters which concern them in accordance with their age and maturity.' The CRC Committee also stresses the importance of engaging a diverse group of children 'when developing legislation, policies, programs, services and training on children's rights in relation to the digital environment.'[88]

While consultation with children and young people on the entirety of the proposed Regulation would be ideal, participants identified the issue of consensual sexual exploration between adolescents and the proposed Regulation thereon as an area where consultation with a diverse group of children and adolescents would be most beneficial to ensure that their views are at the centre of the formulation of such EU legislation.[89]

EFFECTIVENESS OF PROPOSED REGULATION IN ADVANCED TECHNOLOGIES

One participant expressed doubts that the proposed Regulation would be sufficient to police the Metaverse and advanced digital technologies like decentralized versions of online gaming. The Metaverse is a hybrid online/offline environment whereby users are required to use virtual reality (hereafter 'VR') or augmented reality (hereafter 'AR') headsets designed to host sensors, built-in cameras, microphones, and speakers, to enter the Metaverse. Users often adopt personas to engage with others, with little oversight or control of the characters adopted to visually represent their persona. This opens a new arena for criminal activity by adults pretending to be someone else to solicit a child. The Metaverse concept poses many regulatory challenges, especially to the policing of verbal, as opposed to typed messages, between adults and potential child victims. More worryingly, the Metaverse experience is much closer to typical forms of human communications we encounter in the offline world, while the Metaverse environment is designed in a way that preserves characteristics of the online context: anonymity, confidentiality, customization, etc. It is unclear if the proposed Regulation is meant to be applicable to the Metaverse; however, if included, a platform would have to intercept, scan, and analyse private audio communications in real time against the EU Centre's database of indicators. This raises fundamental questions about private actors intercepting private conversations. The EU Commission should consider whether the online CSA offences, as defined in the CSA Directive, capture the diverse forms of online CSA possibly committed in the Metaverse and address any gaps in the upcoming amendment of the CSA Directive. This is an important first step since the proposed Regulation only applies to criminal offences as defined in the CSA Directive.[90]

[88] CRC Committee, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, adopted on 24 March 2021, para. 18.

[89] This need for consultation was also raised by children who participated in the Lanzarote Committee's monitoring round, see Council of Europe, *The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs) - Addressing the challenges raised by child self-generated sexual images and/or video (Implementation Report)*, Strasbourg 10 March 2022.

[90] See Art 2 proposed Regulation.

Metaverses can be designed with two architectures in mind: first, the centralized model where the environment is designed and controlled by a central actor like Meta's Metaverse. In this instance, Meta would be clearly subject to the obligations found in the proposed Regulation. However, other platform architectures with no clear 'central authority' exist. These decentralized platforms, like Mastodon, require a rethink about how the proposed Regulation would apply. On Mastodon, each user is a member of a specific server, which interoperates with each other as a federated social network, allowing users on different servers to interact. Does the proposed Regulation, therefore, apply to each user's server? As of 18 November 2022, Mastodon has over seven million users operating across independent, decentralized service providers.

5.2 IDENTIFYING COMMON GROUND

All participants made clear that the problem of online CSA was multi-dimensional, besotted with societal challenges. Some expressed concern that the proposed Regulation lacks the necessary multi-sectoral and holistic response. In contrast, others acknowledged that this was partly because it was not the aim of this legal instrument, referring notably to the CSA Directive. Some participants expressed concern about the 'techno-solutionism' imposed by the proposed Regulation when the problem of online CSA was multi-faceted and multi-layered. While participants generally agreed that there was a significant need for further interrogation of a variety of issues, there was also some common ground among the participants of how the EU could take regulatory steps to prevent and respond to online CSA. Please note that the below areas of common ground are not listed in an order of priority and should hence all be considered equally important:

- **Risk assessment**: the proposed risk assessment specifically for online CSA was largely perceived as beneficial. It should be coupled with a more comprehensive human rights impact assessment and intricately linked to the DSA.
- **Mandatory reporting of illegal content**: participants agreed that providers should have a legal obligation to report illegal content such as online CSA. The current liability regime was considered insufficient.
- **Prevent reporting of the content of consensual sexual exploration between adolescents to law enforcement:** participants agreed that adolescents should not face prosecution for consensual sexual exploration, under specific circumstances.
- **Less intrusive measures**: less intrusive measures, which providers could notably adopt as part of risk mitigation measures imposed by the proposed Regulation, should also be further considered, and, when relevant, clearly mandated by the proposed Regulation, as part of a more comprehensive approach to the problem of online CSA.
- **Child-friendly reporting mechanisms:** participants proposed the setting of mandatory standards for child-friendly reporting mechanisms on platforms, to ensure that they are easy to find and use; clear and timely feedback mechanisms should be a mandatory feature of such a reporting mechanism; children should be involved in the design process of such reporting mechanisms.
- **Certain functions of the EU Centre:** most participants agreed that the EU Centre should be independent of EUROPOL to clearly demarcate functions to law enforcement; it should serve as a platform for knowledge sharing and coordination and EU-wide victim support.

- **Better funding and capacity building for law enforcement**: alongside clear lines of demarcation for law enforcement agencies and the EU Centre in their working relationship with EUROPOL, participants agreed that national law enforcement agencies face considerable financial and technical capacity constraints which need to be addressed as a matter of urgency.
- **Clear legal mandate and guaranteed funding for hotlines:** participants agreed that hotlines should have a legal mandate to report cases directly to the EU Centre and stressed that due to the key role they play in the overall child rights ecosystem, funding for hotlines should be secured through the proposed Regulation.
- **Mental health support for content moderators involved in online CSA assessment:** participants acknowledged the traumatizing impact the assessment of online CSA can have on content moderators and asked for mental health support for such moderator.
- **Discriminatory impact of proposed Regulation, including on marginalized groups and linguistic minorities:** participants highlighted the need for extensive research into how such technology would function across the EU's 24 official languages and the potentially discriminatory impact of the proposed Regulation, including on marginalized groups and cultures, extending for instance to how automated technologies impact those who speak something other than English as their first language.
- **Clearer criteria for technology deployed under the proposed Regulation**: participants agreed that there should be more clarity on the criteria, thresholds and assessment process for the technology used for the implementation of the proposed Regulation.
- Integration of a **victim-centred approach** and considerations when notifying the sender of illicit content and how the experience affected them.

The Workshop was not tasked with producing concrete solutions to problems, nor recommendations on how to remedy issues with the proposed Regulation. It emerges from the discussion that there remain clear contentious elements of the debate. For instance, there were clear issues with what privacy advocates in attendance characterized as a mandate to create a blanket surveillance program over users' communications. Some participants would never agree to the type of monitoring envisaged in the proposed Regulation that would allow scanning all private communications looking for indicators of CSAM and solicitation of children. However, others argued that such a program was possible and required for the prevention and response to online CSA but could not (in the legal sense) and should not (in the moral sense) be implemented without clear procedural rules and additional safeguards and protections. While it is arguably unlikely that participants will change their respective views about this substantive question, it was helpful to discuss with participants which common ground they could identify and could jointly support.

6. CONCLUSION

The Expert Workshop on the EU proposed Regulation on preventing and combatting child sexual abuse brought together experts in law and regulatory theory, privacy, and data protection and child rights experts from across the EU. The workshop's objective was to search for common ground between disciplines that have a stake in the proposed Regulation's implementation. There is a (mis)perception that privacy/data protection/data security experts sit in stark opposition to the objective of using the law to protect children from the monstrosities of exploitative production and distribution of CSAM and solicitation of children. The question before the workshop was simple: can we find agreement in some aspects of the proposal that might close the gap between the two sides?

There was unequivocal consensus among all workshop participants that the ease of proliferation and dissemination of CSAM is amplified by the technical characteristics of digital technologies. There is even some suggestion that the fundamental rights to privacy and data protection at the heart of European law make it appreciably easier to host CSAM within the borders of Europe. Participants also endorsed the need for a holistic multi-sectoral prevention and response strategy to online CSA. Further, participants found common ground regarding some regulatory measures such as online CSA specific risk assessments, the role of the EU Centre as independent body tasked with knowledge sharing and coordination amongst EU Member States, clear guidelines for establishing child-friendly reporting mechanisms and better funding and capacity building for law enforcement agencies (see section 5.2 for more details on the common ground).

Finally, there was a universal agreement that we need to continue these workshops. As this workshop laid the groundwork for discussion and served as a platform for further deliberation amongst a diverse group of experts, it was also obvious that some issues were not sufficiently discussed and that additional issues were not covered in the available time frame.

As one participant stated:

> "I *know this proposal was complex, but I had no idea it was this complex*."

Another participant explained their frustrations about the proposed Regulation a little differently:

> "W*e have only really been talking about the implications of the proposal on platforms that run an open and centralized architecture; however, we need to talk about the implications for those running end-to-end architecture and requirements to put in a back-door to scan private communications.*"

Many participants observed that it was impossible to determine the implications for fundamental rights because there was no discernible pathway for what happens after *new* CSAM, or potential solicitation of children was flagged for additional review by the EU Centre. We offer ten questions that require further investigation and clarity by the Commission going forward:

> "*How many professionals on the side of providers and law enforcement agencies would review flagged materials?"*
>
> *"What happens procedurally after a flagging? A review?"*

"What will law enforcement do after notification of potential solicitation of a child?"

"What safeguards are there for the adult/child falsely flagged by an AI system?"

"How can the rights of appeal as set out in the proposed Regulation be simplified and made more meaningful for all affected parties?"

"In instances where inappropriate/unlawful behaviour is taking place, how quickly can this system instigate support for the child victims?"

"As the proposed Regulation leads to the mandatory introduction of age verification and/or age assessment measures on some products/services, which procedural and substantive safeguards does the EU envisage to ensure such tools do not violate fundamental rights?"

"What protections are there for consensual sexual exploration between adolescents and consensual sexual exploration between an adolescent and their adult partner of similar age and maturity?"

"How and which information will be shared between the EU Centre and EUROPOL and national law enforcement agencies?"

"Is it possible to deploy the detection, reporting and blocking system across either centralized or decentralized platforms that protect the privacy of communications through end-to-end encryption and what is the impact on fundamental rights?"

To answer some of the above questions, any further workshop would benefit from additional expertise from both those working on cybercrime and with law enforcement agencies on the reporting and policing of CSAM and solicitation of children, especially those with experience implementing and overseeing procedural safeguards.

This workshop was a first attempt to bridge the gap between child rights and privacy and data protection advocates which often have fundamentally different positions when it comes to the role of providers and technology in the prevention and response to online CSA. All participants of the workshop were in attendance because of their unwavering belief in the importance of finding proportionate solutions to online CSA that respect and protect the fundamental rights of all users - children and adults alike. We hope that future workshops on the areas identified in section 5.1 for further interrogation will carry the same collegial spirit and serve as a platform for knowledge sharing, critical reflection and learning and help to develop evidence-based, informed EU laws and policies.