

**BALANCING  
THE RIGHT TO  
PRIVACY WITH  
THE CHILDREN'S  
RIGHT TO  
PROTECTION FROM  
ONLINE SEXUAL  
EXPLOITATION**

# TABLE OF CONTENT

<b>Table of Abbreviation</b>	<b>3</b>
<b>1. Introduction: Context</b>	<b>4</b>
1.1 Research aim: striking a balance between child protection and online privacy rights	5
1.2 Research methodology	6
1.3 Limitations	6
<b>2. The Proposed CSA Regulation</b>	<b>7</b>
<b>3. Detection Tools and privacy implications</b>	<b>10</b>
<b>4. Human rights at play</b>	<b>14</b>
4.1 Overview of the Applicable Legislation	16
4.2 The Right to the Respect for Private Life	17
4.3 The Protection of Children from OCSE	19
<b>5. Striking a balance</b>	<b>21</b>
5.1 Provided for by Law	23
5.2 Respecting the Essence of the Right Concerned	24
5.3 Objective of General Interest	26
5.4 Respect the Principle of Proportionality	27
A. Appropriateness of the measures	27
B. Necessity of the measures	28
C. Proportionality stricto sensu of the measures	31
<b>6. Findings and recommendations</b>	<b>33</b>
<b>Annex 1: Glossary</b>	<b>35</b>
<b>Annex 2: Potential viable CSAM detection technologies</b>	<b>37</b>

# TABLE OF ABBREVIATIONS

<b>CJEU</b>	Court of Justice of the European Union
<b>CSAM</b>	Child Sexual Abuse Material
<b>E2EE</b>	End-to-End Encryption
<b>ECHR</b>	European Convention on Human Rights
<b>ECtHR</b>	European Court of Human Rights
<b>EU</b>	European Union
<b>EU Charter</b>	Charter of Fundamental Rights of the European union
<b>ICTs</b>	Information and Communication Technologies
<b>IWF</b>	The Internet Watch Foundation
<b>OCSE</b>	Online Child Sexual Exploitation
<b>Proposed CSA Regulation</b>	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 2022/0155
<b>UNCRC</b>	United Nation Convention on the Rights of the Child

# 1. Introduction: Context

The development of information and communication technologies (ICTs)<sup>1</sup>, including Artificial Intelligence (AI), brings a new era of opportunities, including for children to learn, play and socialise. However, these technologies also offer new opportunities to criminals, including sex offenders. ICTs have **increased children's vulnerability to sexual exploitation**, enabling sex offenders to easily establish connections with and manipulate children, livestream child sexual abuse, and share child sexual abuse material (CSAM), including AI-generated material<sup>2</sup>.

In 2023, NCMEC's CyberTipline<sup>3</sup> received reports of suspected child sexual exploitation from US-based online social media platforms amounting to **105.6 millions** images or videos containing child sexual abuse (CSA)<sup>4</sup>. The Internet Watch Foundation (IWF) found 275,652 webpages containing child sexual abuse imagery, and, for the first time, the IWF received reports of children as young as **three to six years old groomed** to capture sexual imagery of themselves<sup>5</sup>. From September 2023 to March 2024, the IWF analysed AI-generated CSAM and found a significant increase in "hard core" images, rising by 10 percentage points. This increase indicates that technological advancements and improved expertise are allowing perpetrators to create more sophisticated and explicit content<sup>6</sup>. These numbers are only based on what has been reported by the public and some platforms, which means it is only the **tip of the iceberg**. The volume of CSAM is believed to be much higher than what is currently known. For instance, in the Netherlands, an estimated 68% of

children have experienced sexual harm online<sup>7</sup>. Just because adults may not encounter CSAM online does not mean that children are not experiencing it. In fact, research shows that **children tend to develop a high tolerance for online risks**, accepting them as an inherent part of their digital experience, leading them not to disclose what they actually encounter online or to seek help from adults<sup>8</sup>.



1 "Information and communication technology, abbreviated as ICT, covers all technical means used to handle information and aid communication. This includes both computer and network hardware, as well as their software." [EU Glossary](#).

2 UN Committee on the Rights of the Child, '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' (10 September 2019) UN Doc CRC/C/156 (CRC Guidelines on the OPSC) para 2.

3 NCMEC's CyberTipline is a nation's centralised reporting system for the online exploitation of children in the United States.

4 NCMEC, [CyberTipline 2023](#).

5 Internet Watch Foundation, ['The Annual Report 2023: #BehindTheScreens'](#).

6 Internet Watch Foundation, [What has changed in the AI CSAM landscape?](#), July 2024.

7 WeProtect Global Alliance, [Estimate of childhood exposure to online child sexual abuse](#) (the Netherlands).

8 Eurochild, Ecpat International, Terre des Hommes Netherlands, (2024). [Speaking Up for Change: children's and caregivers' voices for safer online experiences](#).

9 Ibid.


Tracking the true extent of the dissemination of CSAM and situations of grooming has proven challenging due to multiple factors. These include the inaccessibility of CSAM and grooming which are often taking place in **end-to-end encrypted** (E2EE) networks<sup>10</sup>. Recent research led by Protect Children shows that E2EE messaging apps are massively used to search for, view and share CSAM. Encrypted messaging apps are often favoured by offenders due to the security and privacy offered by E2EE, which allows them to commit crimes without fear of detection<sup>11</sup>. As service providers implement end-to-end encryption in their design choices, the current techniques become less effective, and some methods, such as standard servers checking whether images are known child sexual abuse material, no longer function<sup>12</sup>. Other factors include the sheer **volume** of online material, the use of **AI** technologies to create CSAM or the **fragmented information** scattered among different entities such as law enforcement authorities, hotlines, and electronic service providers<sup>13</sup>.

The ever-evolving nature of the internet poses growing difficulties in tackling these offences<sup>14</sup>. Due to the voluntary nature of existing measures, the EU policy-makers decide to attempt legislating it. In May 2022, the European Commission adopted a **proposal for a Regulation 'laying down rules to prevent and combat child sexual abuse'**<sup>15</sup> (here after "*the Proposed CSA Regulation*" or "*the Proposal*") to tackle the issue. The Proposal aims at curbing online child sexual abuse holistically by, among others, setting obligations for hosting or interpersonal communication services operating in the European Union (EU):

1. **To evaluate the risk** of their service being used for online CSA<sup>16</sup>, and;
2. **To detect** such content<sup>17</sup>, based on an administrative or judicial order, if the mitigation measures prove insufficient to tackle CSAM<sup>18</sup>.

## 1.1 Research aim: striking a balance between child protection and online privacy rights

Despite voluntary detection not having shown any problematic impact on privacy rights, the Proposed Regulation has sparked significant controversy, with privacy rights organisations and activists expressing concerns about its potential impact on the fundamental right to private life in light of the mandatory approach taken by the European Commission's proposal<sup>19</sup>. This research aims to determine:

 Whether the protection of children from online child sexual exploitation (OCSE) can constitute a **legitimate justification** for a potential restriction of the right to online privacy under human rights law. In simpler terms, the report will assess whether a restriction on the right to privacy can be justified (**justification assessment**) and to what extent such a limitation is reasonable (**proportionality assessment**).

<sup>10</sup> Protect Children, '[Tech Platforms Used by Online Child Sexual Abuse Offenders. Research Report with Actionable Recommendations for the Tech Industry](#)', February 2024.

<sup>11</sup> Protect Children, '[Tech Platforms Used by Online Child Sexual Abuse Offenders](#)', February 2024.

<sup>12</sup> Dr I. Levy, C. Robinson, 'Thoughts on Child Safety on Commodity Platforms' (2022).

<sup>13</sup> M. Dorotic, J. W. Johnsen, 'Child Sexual Abuse on the Internet: Report on the Analysis of Technological Factors That Affect the Creation and Sharing of Child Sexual Abuse Material on the Internet.' (BI Norwegian Business School 2023) Research Report 1.

<sup>14</sup> UNDOC, 'Online Child Sexual Exploitation and Abuse'.

<sup>15</sup> European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' [COM \(2022\) 209 final](#) (here after "*Proposed CSA Regulation*").

<sup>16</sup> Proposed CSA Regulation, art 3.

<sup>17</sup> Proposed CSA Regulation, art 7.

<sup>18</sup> Proposed CSA Regulation, art 12.

<sup>19</sup> L. Bertuzzi, M. Killeen, 'Fact-checkers call out Commission on anti-child abuse material proposal', Euractiv, 2 February 2023.



Whether the proposed regulatory framework offers the required safeguards to guarantee the restrictions on the right to privacy are limited to what is necessary following an adequate balancing of rights exercise.

In order to make this assessment, we will be guided by the criteria set by the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

## 1.2 Research methodology

The research method used in this report combines doctrinal research with an in-depth and systematic analysis of relevant case law of the CJEU and the ECtHR, in connection either with Article 7 of the EU Charter or with Article 8 of the European Convention on Human Rights (ECHR). The doctrinal research involved gathering and analysing different types of legal and non-legal sources with a view to obtaining an overview of the relevant legal rules and their practical application. This method suited the aim of the report as it offers a comprehensive overview of the applicable legal standards and scope of both the right to online privacy and of the children's right to be free from OCSE. The doctrinal and case-law research is supplemented by relevant literature. The perspective of children is brought throughout thanks to the VOICE research<sup>20</sup> which consulted children on the issue of balancing privacy rights and online safety of children.

## 1.3 Limitations

This research assesses the compliance of the Proposed CSA Regulation with human rights law, focusing on the right to privacy as a key consideration. This research is based on our own interpretation of the case law of the CJEU and the ECtHR, meaning that the conclusions drawn reflect our understanding of the Courts' decisions.

It acknowledges that a comprehensive evaluation would require inclusion of the right to data protection, which is a distinct yet interconnected right under human rights law<sup>21</sup>. The right to data protection, enshrined in Article 8 of the EU Charter, imposes obligations on those who process personal data. The General Data Protection Regulation<sup>22</sup> (GDPR) is the legislative framework that operationalise the principles laid out in Article 8 of the EU Charter and that provides a specific legal basis for processing personal data, ensuring that data protection is upheld in practice<sup>23</sup>. This report does not delve into the nuances of these legal bases, nor does it evaluate the Proposed CSA Regulation against the full spectrum of data protection rights. However, we acknowledge the necessity for detection orders to have a solid legal basis in accordance with the GDPR to ensure the lawful execution of CSAM detection.

<sup>20</sup> Ibid.

<sup>21</sup> G.González Fuster and H. Hijmans, '[The EU rights to privacy and personal data protection: 20 years in 10 questions](#)', Brussels Privacy Hub.

<sup>22</sup> 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 ( here after 'General Data Protection Regulation').

<sup>23</sup> General Data Protection Regulation, Art. 6.

## 2. The Proposed CSA Regulation Context



### KEY FINDINGS

1

The Proposed CSA Regulation establishes a standardised legal framework to address children's right to be protected from online sexual harm, while addressing the concerns on the right to privacy involved in the methods of tackling OCSE.

2

It mandates the use of detection technologies through orders issued by competent authorities, balancing privacy and combating CSAM within a strict framework.

3

The Proposed CSA Regulation is set up to look at the privacy rights implication of detection tools, little is said about looking at the child rights implications of the dissemination of OCSE.



**“[We must] create a legislation in which all sites are safe and punish those that don't comply.”**

(VOICE research, Children from Portugal)

and their specific risks associated with online child sexual abuse. This would be achieved by requiring each platform to undertake a **risk assessment** of the risk of OCSE on their service and to adopt **risk mitigation** measures, such as safety by design features<sup>25</sup> (e.g. effective age verification methods, high privacy settings by default), to address the identified risks.

The 2022 Proposed CSA Regulation was designed to effectively combat online child sexual abuse by establishing a **standardised legal framework** that applies throughout the EU<sup>24</sup>.

The Proposal outlines measures which purposed to address OCSE holistically, tailored to each platform

The European Commission's proposal also introduced the possibility for the **mandatory use of detection technologies** by providers of electronic communication and hosting services, which carry significant risks of online CSA<sup>26</sup>. The incorporation of detection order procedure in the proposal stems from the voluntary use of these technologies for over

<sup>24</sup> Proposed CSA Regulation.

<sup>25</sup> In the final section of this report, we emphasise the necessity of adopting a child safety by design approach. Safety by design is a user-centred approach that puts user safety and rights at the core of the design and development of services and products. These design features can help prevent OSEC by excluding predators from children's online forums and ensuring age-appropriate online experiences for young users. See Down to Zero Alliance, (2022). [Child safety by design that works against online sexual exploitation of children](#).

<sup>26</sup> Proposed CSA Regulation, art. 7 to 11.

a decade. Due to the disparity in the deployment of such detection technologies across platforms and in order to build oversight over such detection, the proposed Regulation mandates through a detection order system, whereby a competent judicial authority or an independent administrative authority would issue such **detection order** following a request by a Coordinating Authority (designated by a Member State) when there is:

1. A significant risk of the service being used for the

purposes of online child sexual abuse and;

2. The reasons for issuing the order “*outweigh the negative consequences for the rights and interests of all parties affected*”.

Furthermore, an EU Centre would assist in implementing the Regulation and address challenges related to detecting, reporting, and removing online child sexual abuse material<sup>27</sup>. An overview of the detection order procedure is presented below.

Figure 1. Overview of a CSAM Detection Order under the Proposed CSA Regulation



27 Proposed CSA Regulation, art. 40 to 82.

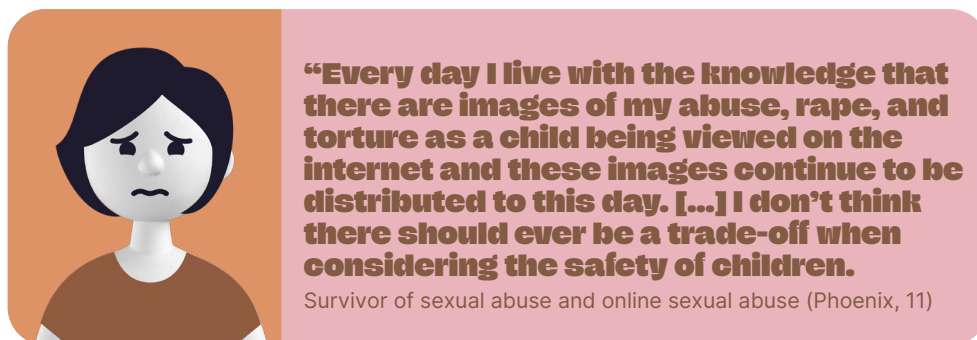


By assigning the task of balancing fundamental rights to judicial or independent administrative **authorities instead of private companies**, as it is currently the case, the Proposed CSA Regulation serves as a strong safeguard for the protection of the right to private life.

As the above overview of the Detection Order process shows, the Proposed Regulation is heavily concerned with the privacy implications of detection technology. To mitigate those potential privacy implications, it establishes a comprehensive process, including the requirement to carry out a data protection impact assessment, to minimise interference with privacy rights. However, upon closer analysis of the Proposed Regulation, it becomes evident that **there is no similar requirement for the implications on children's rights**.

The Proposal has insufficient attention given to how this balancing of rights will address children's rights to protection from OCSE. For instance, **no child right impact assessment is mandated nor the intervention of any child rights Ombudsperson or body foreseen**. Regarding the EU Centre, its expertise seems to be primarily focused on the technological aspects of detection through a Technology Committee, rather than on a thorough understanding of children's rights. The Proposed Regulation also fails to consider children's right to privacy, specifically their protection against the non-consensual dissemination of images depicting them.

As of July 2024, the Proposed CSA Regulation remains in the proposal stage, and the legislative process is still ongoing.



# 3. Detection Tools and Privacy Implications



## KEY FINDINGS

1

Detection tools represent the primary viable option to detecting child sexual abuse offences online at scale, as law enforcement faces significant challenges in achieving comparable effectiveness to the volume in circulation.

2

CSAM detection tools have been safely deployed for over a decade.

3

CSAM detections tools are unable to comprehend users' communications and its functions are strictly limited to flagging the likelihood of criminal material being present on a service. Therefore, mass surveillance claims are unfounded.

4

A safe online environment for children that effectively combats child sexual abuse online can be ensured by using detection tools as part of a safety by design approach.

5

Privacy and child protection should be seen as complementary rather than trade-offs.



**“We believe that the detection mechanism should be used because some children below 13 can make accounts on social media and they could be influenced by adults to [participate] in sexual affairs and to receive inappropriate photos.”**

(VOICE research, Children from Romania)

The Proposed CSA Regulation **does not specify which technologies must be employed** in the execution of detection orders but only sets out the criteria to be used in selecting suitable detection technologies<sup>28</sup>. Before delving into the legal assessment of the Proposed CSA Regulation, it is important to understand the technologies that might be used if the Regulation was enacted. To this end, we will look at some of the existing technologies used to detect CSAM, based on publicly available information. We caveat the below information to the fact that technology is not fixed and can be tailor made depending on the objectives. In addition, technologies evolve fast and new technologies in this field continue to be created and tested.

28 Proposed CSA Regulation.

Currently, CSAM detection falls under the category of automated content scanning, representing a technology designed for the automated scanning of users' communications (or part of communication). CSAM detection technology does not comprehend or interpret the content of users' communications. Instead, it is trained to find keywords or to evaluate images and videos as to whether there is CSAM or not. In short, the technology does not 'know' what the image features specifically, it is trained to say whether or not it is CSAM.

For known CSAM, it compares digital fingerprints through **hash-matching** against a database of already confirmed CSAM. Regarding unknown CSAM, it employs a **machine learning classifier** to assess the likelihood that a content is CSAM. The technology will provide a percentage probability that it is CSAM. The machine learning classifiers are trained based on confirmed CSAM database, adult pornography and benign images of children in order to make the difference between criminal material and innocent material. Subsequently, content flagged by the classifier undergoes a **multi-step verification process**, including human review, to confirm its classification as CSAM.

In summary, these tools and technologies do not engage in data collection or analysis of the content of images and videos beyond determining the presence of CSAM: **their function is strictly limited to the identification of criminal material and they are only able to recognise patterns indicating a CSAM**<sup>29</sup>.

As we explore the potential viable CSAM detection technologies, **four essential points** should be kept in mind.

**Firstly**, detection technologies play an important role in combating the spread of CSAM by enabling the identification and removal of harmful content,

ultimately leading to the rescue of children and the apprehension of sex offenders. As stated in the Joint Declaration of the European Police Chiefs at Europol, "[...] companies currently have the ability to alert the proper authorities - with the result that many thousands of children have been safeguarded, and perpetrators arrested and brought to justice"<sup>30</sup>. Detection technologies have a **tangible impact in safeguarding children and holding offenders accountable**, leveraging them is essential in the fight against OCSE<sup>31</sup>.

**Secondly**, a 2022 study by Pfefferkorn revealed a widespread consensus among online service providers regarding the **effectiveness** of automated content scanning, particularly in detection of CSAM<sup>32</sup>. This is particularly important considering the inherent limitations of police investigations in addressing these online threats. These limitations include resource constraints and the impracticality of having law enforcement review all communication to identify CSAM. According to Europol, the volume of online CSAM in the EU has become simply unmanageable for many of the law enforcement units dealing with it<sup>33</sup>. The high number of reports made by US-based companies (no less than 105.6 million in 2023)<sup>34</sup> underscores the impossibility for police to tackle this issue at scale. With many national police forces already inundated by reports from organisations like NCMEC, the feasibility of effectively managing such a vast number of reports without technology is questionable. In light of these constraints, there is a clear need for wider adoption of CSAM detection technologies<sup>35</sup>. Without detection technology, law enforcement would only rely on public reports, which is significantly lower. Since in 2023, the NCMEC CyberTipline received only 265,542 reports from the public, whereas online service providers submitted over 35,944,826 reports<sup>36</sup>. The IWF 2023 Annual Report reveals a similar discrepancy between proactive research,

29 In the attached annex 2, we explored the potential viable detection technologies to gain a more comprehensive understanding of their capabilities in combating online child sexual abuse.

30 Europol (2024). [Joint Declaration of the European Police Chiefs](#).

31 UK Government, [End-to-end encryption and child safety](#), 2023. According to the National Crime Agency in the United Kingdom, the information that social media companies give to UK law enforcement contributes to over 800 arrests of suspected child sex offenders, and results in an estimated 1,200 children being safeguarded from child sexual abuse on average every month.

32 Pfefferkorn, R. (2022). [Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers](#). Journal of Online Trust and Safety, 1(2).

33 Europol, ['Internet Organised Crime Threat Assessment \(IOCTA\)'](#), 2020.

34 NCMEC, [CyberTipline 2023](#).

35 CSAM detection technologies have been safely and effectively deployed for over a decade, e.g. PhotoDNA was developed in 2009.

36 NCMEC, [CyberTipline 2023](#).

where IWF analysts search for CSAM, and CSAM reports from external sources, including public reporting<sup>37</sup>. This stark contrast highlights two key points. First, it underscores the inadequacy of public reporting alone, revealing various barriers to reporting that need to be addressed, but will never be fully overcome<sup>38</sup>. Second, it demonstrates that public reporting is insufficient and that the removal of illegal content from the online world largely depends on proactive searches for CSAM using detection tools. For instance, the Canadian Project Arachnid, an automated web crawling detection tool designed to identify known CSAM or similar content, processed more than 168 billion images from 2017 to May 2024. During this period, it flagged 75 million pieces of suspicious media for analyst review and issued 39 million takedown notices. This project underscores the effectiveness of proactive searches in identifying CSAM on a scale that corresponds to its widespread circulation<sup>39</sup>.

**Thirdly**, the recent report from the European Commission on the implementation of Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC emphasises the **high accuracy rate**, exceeding 90%, of new CSAM detection tools. Drawing on data provided by Thorn, the Commission's report also indicates that CSAM classifiers can achieve a precision rate of 99% for both known and unknown CSAM, resulting in a minimal 0.1% false positive rate. For instance, PhotoDNA, a popular hash technology used to combat known CSAM<sup>40</sup>, has a false positive rate of less than one in one trillion<sup>41</sup>.

In other areas of our society, the use of technology for crime detection has been widely accepted, such as AI automated detection of bank transactions for money laundering and fraudulent behaviour<sup>42</sup> or more well-known speed radars. In comparison, a study led in 2016 showed that speed radars had error rates of 1.5% to 2.1% in detecting speeds<sup>43</sup>. Despite these inaccuracies, speed radars are widely deployed for road safety because the benefits outweigh the small margin of error.

**Finally**, and again as outlined in the Commission's report, the list of technologies mentioned as a means to combat online child sexual abuse is not exhaustive. This means that other detection tools that are privacy preserving may also reach a high level of accuracy or may be developed in the future. The Regulation by requiring a high level of privacy protection will act as incentive to developers and companies to ensure high accuracy level and privacy preserving techniques are deployed. In addition, similar technology is already deployed for purposes other than preventing online child sexual abuse, such as to fight against the online terrorist content<sup>44</sup>, online banking fraud or existing malware online<sup>45</sup>.

**“With the terrorist EU legislation, platforms are required to remove terrorist materials in less than one hour, why don't we apply this in case of sexual abuse of minors?”**

Spanish Data Protection Authority Director<sup>46</sup>.



37 Internet Watch Foundation, 'The Annual Report 2023: #BehindTheScreens'.

38 We elaborate further on those barriers below.

39 Project Arachnid.

40 For further explanation, see Annex 2.

41 False positive rates refer to the percentage of non-CSAM images or videos that are incorrectly identified as CSAM by the hashing algorithm. False negative rates refer to the percentage of CSAM images or videos that are falsely identified as non-CSAM. See, M. Steinebach, [An Analysis of PhotoDNA](#). In The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29--September 01, 2023, Benevento, Italy. ACM, USA.

42 Jullum, M. et al (2020). [Detecting money laundering transactions with machine learning](#), Journal of Money Laundering Control, Vol. 23 No. 1, pp. 173-186. Example of solution: Snappt. [How AI is Being Used in Fraud Detection](#).

43 Hemin J. Mohammed, Steven Schrock and Eric J. Fitzsimmons (2016), [The accuracy of traffic speed and volume data detected using radar technology](#), Transportation Research Board 95th Annual Meeting.

44 Regulation (EU) (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

45 WhatsApp. (n.d.). [FAQ on suspicious link for web and computers](#). María del Mar España Martí Director of the Spanish Data Protection Agency) at the Event "Demystifying Age

46 María del Mar España Martí Director of the Spanish Data Protection Agency) at the Event "Demystifying Age Assurance to Protect Children Online", 17 April 2024, 5Rights Foundation and the European Parliament Intergroup on Children's Rights.

**Technological solutions ensuring both detection while being privacy preserving do exist, the key lies in how these technologies are set up and used.** Rather than being opposed, online safety and privacy should be viewed as complementary, as they are not mutually exclusive concepts but rather complementary pillars of a secure online environment, particularly for children. On the one hand, privacy empowers children to control their personal information, safeguarding their autonomy

and allowing them to explore the digital world without fear of exploitation or intrusion. On the other hand, safety measures protect children from potential risks and harm and shield them from exposure to harmful content, allowing them to navigate the digital landscape with confidence. When used together, privacy and security measures empower the establishment of a secure online environment for children and effectively combat child sexual abuse online.

# 4. Human Rights at Play



## KEY FINDINGS

1

The current legal framework does not require the detection of any OCSE, relying solely on self-regulation (i.e. voluntary detection) and public reports.

2

The ECtHR has recognised the States' positive obligation to proactively respect for the private and family life of children depicted in the imagery disseminated without the consent and used for child sexual abuse offending.

3

The right to private life is not absolute, as for many fundamental rights, limitations may be imposed on its exercise when specific criteria are met.

4

The EU Charter of Fundamental Rights safeguards children through provisions on human dignity, integrity, and child protection.

5

The CJEU aligns Article 7 of the EU Charter and Article 8 of the ECHR in order to ensure a cohesive approach to protecting fundamental rights.

6

Prioritising the privacy rights of victims and survivors is essential in addressing online child sexual abuse effectively.



**“We want privacy AND protection.”**

(VOICE research, Children in the Netherlands)

In the past decades, the right to online privacy has rapidly gained legal recognition and prominence worldwide<sup>47</sup>. Along with it, so have the concerns for the rights of children online<sup>48</sup>. While, on one hand, there is pressure to protect the right to privacy of communication<sup>49</sup>, on the other hand there are calls for OCSE detection and removal, including in private chats<sup>50</sup>.

47 See for example, UN General Assembly Resolution ‘The Right to Privacy in the Digital Age’ (16 November 2016) UN Doc A/C.3.71/L.39/Rev 1; UNGA ‘The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights’ (30 June 2014) UN Doc A/HRC/23/37; Council of Europe, Committee of Ministers, Recommendation CM/Rec(2012) 4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services (4 April 2012); Council of Europe, Committee of Ministers, Recommendation CM/Rec(2012) 3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, 4 April 2012.

48 L. Lazarus et al., [‘Respecting Human Rights and the Rule of Law When Using Automated Technology to Detect Online Child Sexual Exploitation and Abuse: Independent Experts’ Report](#) (Council of Europe 2021).

49 See for example: European Data Protection Supervisor, Proposal to combat child sexual abuse online presents serious risks for fundamental rights (EDPS, 2022).

50 See: ECLAG, [‘European Parliament IMCO Committee draft report threatens children's safety and fails to understand and respond to child sexual abuse online’](#) (ECPAT, 2023).

Currently, some online platforms, driven by self-regulation, detect CSAM on a voluntary basis. This voluntary detection has been the main driver of the high volume of reported CSAM to NCMEC, **reaching 105.6 millions in 2023**<sup>51</sup>. However, relying solely on voluntary detection of CSAM has been proven to be insufficient in protecting children against forms of online sexual harm, since not all online platforms detect both known and unknown CSAM. In addition, it does not meet the volume of CSAM that is actually in circulation online. Almost a third of 105.6 millions reported CSAM come from Meta applications only<sup>52</sup>, as many platforms either solely rely on public reports or limit detection to known CSAM, effectively missing out a high share of CSAM that are in circulation.

Studies show that fewer than half of caregivers felt that these measures sufficiently protect children from OCSEA. Among the dissenters, common concerns included the inconsistent effectiveness of some online safety measures, the possibility of both offenders and children bypassing these protections. In addition, it should be noted that children showed a high tolerance for risk, viewing it as an inherent aspect of using social media. Some children in the research mentioned, for instance, *'getting used to [...] random men who want to connect with them on social media'*<sup>53</sup>.

**"If you want to be safe online, you shouldn't be on social media!"**

(VOICE research, child participant from the Netherlands)



The **current EU framework**, encompassing the e-commerce Directive<sup>54</sup> and the Digital Service Act<sup>55</sup>, foresees the principle of limited liability. Following this principle, hosting providers are not held accountable for the information stored at the request of the user, as long as they lack actual knowledge of illegal activity or content. However, upon obtaining such knowledge or awareness, providers are mandated to take action by removing or disabling the illegal content<sup>56</sup>. Essentially, the EU legal framework does not establish a general obligation to actively monitor their services for illegal activity and to report those to law enforcement. The Digital Services Act nevertheless introduces an obligation for hosting providers to establish a notice and action mechanism, enabling users to report illegal content on the platform such as CSAM<sup>57</sup>. To effectively combat OCSE, policymakers must recognise their duty to safeguard children from online sexual abuse by encouraging CSAM detection across the EU.

51 NCMEC, [CyberTipline 2023](#).

52 NCMEC, [CyberTipline 2023](#). Reports by Electronic Service Providers.

53 Eurochild, Ecpat International, Terre des Hommes Netherlands, (2024). [Speaking Up for Change: children's and caregivers' voices for safer online experiences](#).

54 Directive (EU) 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') (2000).

55 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.

56 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, art. 6.

57 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, art. 16.



## 4.1 Overview of the Applicable Legislation

Both the EU and the Council of Europe frameworks have enshrined the right to privacy and the right to protection from OCSE. The table below summarises these frameworks:

Council of Europe		EU
The Right to Privacy	Article 8 of the ECHR (right to private and family life) <sup>58</sup> .	Article 7 of the EU Charter (right to the respect for private and family life) <sup>59</sup> .
		Directive on privacy and electronic communications <sup>60</sup> .
Protection of Children from OCSE	The Convention on Cybercrime <sup>61</sup> (The Budapest Convention).	Protection of children from OCSE in the Charter of Fundamental rights of the European Union can be inferred from Article 1 EU Charter on the protection of human dignity, Article 3 on the protection of the integrity of the person, Article 4 on the prohibition of inhuman and degrading treatment, Article 24 on the rights of children to have the protection and care necessary for their well-being.
		Regulation 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communication services for the processing of personal and other data for the purpose of combating online child sexual abuse <sup>63</sup> .
	The Convention on the Protection of children against Sexual Exploitation and Sexual Abuse <sup>62</sup> (The Lanzarote Convention).	Article 28 of the Digital Services Act <sup>64</sup> .
		Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children.

58 "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

59 "Everyone has the right to respect for one's private and family life, home and communications."

60 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.

61 Council of Europe, Convention on Cybercrime, 23 November 2001, European Treaty Series - No. 185.

62 Council of Europe, Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, 1 July 2010, CETS No. 21.

63 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC for the purpose of combating online child sexual abuse.

64 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).



## 4.2 The Right to the Respect for Private Life

The obligation to respect people's online privacy falls under the umbrella of the internationally recognised **right to private life**, which is recognised in several human rights conventions<sup>65</sup>. While the concept of privacy has existed in all societies and cultures throughout history, **there is yet no binding and internationally accepted definition of the right to privacy**. Generally, it is agreed that privacy encompasses the extent to which information about an individual is disclosed to the public<sup>66</sup>. In the context of CSA, privacy encompasses safeguarding the privacy of victims by preventing the unauthorised dissemination of their material, while concurrently ensuring the protection of internet users' personal information through guarding against intrusive data processing techniques.

Within the **Council of Europe**, Article 8 ECHR protects the right to respect for private and family life<sup>67</sup>. The ECHR is binding on its 46 States Parties, including all 27 EU Member States, which means they must comply with Article 8 ECHR when implementing the Proposed CSA Regulation, should the Regulation become legally binding in the EU<sup>68</sup>.

Article 8 ECHR entails both positive and negative obligations on Contracting States. Positive obligations require states to actively protect individuals' privacy, while negative obligations require them to refrain from unjustified interference. The below case-law demonstrates the need for positive obligation to identify criminal acts and their offenders, as well as how the **non-consensual dissemination of an image depicting a child is a privacy rights violation first and foremost**.

The case law *K.U. v Finland* is an illustration of the positive obligations regarding Article 8 ECHR incumbent on Contracting States. The applicant, a minor at the time, had his private information and image posted on a dating site without his consent, leading to solicitation from unknown adults. Despite complaints to the police, the service provider refused to disclose the perpetrator's identity. Legal redress was unsuccessful, prompting a complaint under Article 8 for invasion of privacy and lack of an effective remedy under Article 13 ECHR.

In its ruling, the Court reiterates that Contracting states may have **negative<sup>69</sup> and positive obligation** inherent to a **proactive respect for private and family life<sup>70</sup>** and holds that effective deterrence against grave acts, **involving a minor and making him a target for being approached by offenders**, requires efficient criminal law provisions<sup>71</sup>. Public interest and the protection of victims' interest necessitates a remedy enabling the identification and prosecution of offenders, which was lacking in the Finnish domestic law.

The Court found a violation of Article 8 ECHR, emphasising that the deficiency in the legislative framework led to the inability to discharge Finland's positive obligation of protecting the right to private life of the child applicant, which hindered practical protection of the minor. This legal precedent underscores the responsibility of States under Article 8 ECHR to proactively and effectively safeguard the privacy of children.

65 Council of Europe, 'Right to privacy'.

66 C. Braghin and M. Cremonini, (2017). Online Privacy. Computer and Information Security Handbook.

67 "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

68 Convention for the Protection of Human Rights and Fundamental Freedoms (here after "ECHR").

69 Meaning that States should abstain from any interference.

70 ECtHR, *K..U. v. Finland*, 2 December 2008, pt. 42.

71 ECtHR, *K..U. v. Finland*, 2 December 2008, pt. 43-45.

Within **the EU**, Article 7 of the **EU Charter** protects the right to respect for one's private and family life, home and communications<sup>72</sup>. This article is explicitly derived from Article 8 ECHR<sup>73</sup>.

The right to privacy is not absolute. In fact, under **Article 52(1)** of the EU Charter, **limitations may be imposed on the exercise of the rights** contained within the Charter on the condition that they are provided by law, respect the essence of those rights and freedoms, and are, subject to the principle of proportionality, *"necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"*<sup>74</sup>.

The alignment between the protection regime of Article 7 of the Charter and Article 8 of the ECHR, although the wording may differ slightly, ensures a **cohesive approach** to safeguarding fundamental rights across European legal frameworks. This will be ensured by the **CJEU**.

Since 2009<sup>75</sup>, the EU Charter has emerged as the primary reference for evaluating the conformity of EU secondary law (such as the Proposed CSA Regulation) with fundamental rights. CJEU case law established that, as the EU has not acceded yet

to the ECHR, it is not a legal instrument which has been formally incorporated into EU law<sup>76</sup>. Therefore, the CJEU will assess the Proposed CSA Regulation according to the EU Charter<sup>77</sup>. This assessment will take into consideration the certain provisions of the ECHR for the purpose of interpreting the EU Charter<sup>78</sup>. Accordingly, the rights of the Charter corresponding to the rights of the ECHR shall be given the same scope and meaning, in order to prevent EU law from providing more extensive protection<sup>79</sup>. This means that the Charter's provisions that derive from the ECHR should be interpreted in the light of the case law of the ECHR, including permissible limitations<sup>80</sup>.

In terms of secondary legislation, the EU Directive 2002/58/EC on e-Privacy and electronic communications (hereafter, **The e-Privacy Directive**) mandates Member States to ensure that an individual's confidentiality of communications and traffic data is respected<sup>81</sup>. Internet service providers must comply with the e-Privacy Directive and adhere to the conditions for processing communications data. The e-Privacy Directive posed a challenge for online service providers seeking to engage in voluntary detection, as it mandates ensuring the confidentiality of communications and related traffic data as a general rule<sup>82</sup>.

72 "Everyone has the right to respect for his or her private and family life, home and communications."

73 The European Parliament, Council and Commission (2002), Explanations to the Charter. The explanations explicitly identify Article 7 as a right derived from Article 8 ECHR, which should be read accordingly. For a case law application, see CJEU, C-578/08, *Rhimou Chakroun v Minister van Buitenlandse Zaken*, 4 March 2010, pt. 44, in which the Court mentions both Article 8 ECHR and Article 7 CFR as sources of the right to private life.

74 Charter of Fundamental Rights of the European Union [2007] OJ C303/1 (here after "EU Charter"), art. 52(1).

75 1 December 2009 is the date of entry into force of the Treaty of Lisbon. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007)

76 CJEU, C-617/10, *Åklagaren v Hans Åkerberg Fransson*, 26 February 2013, pt. 44 ; CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016, pt. 127-129.

77 CJEU rulings have emphasised that an assessment of the legality of a provision of secondary EU legislation *"must be undertaken solely in the light of the fundamental rights guaranteed by the Charter"*, see CJEU, C-199/11, *Europese Gemeenschap v Otis NV and Others*, 6 November 2012, pt. 47 ; CJEU, C-398/13 P, *Inuit Tapiriit Kanatami and Others v Commission*, 19 March 2015, pt. 46.

78 Art. 6(3), Consolidated version of the Treaty on European Union (TEU), 2008/C 115/01, European Union, 13 December 2007, which states that *"Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law"*. For an application, see CJEU, C-601/15 PPU, *J. N. v Staatssecretaris van Veiligheid en Justitie*, 15 February 2016, pt. 77.

79 EU Charter, art. 52(3).

80 According to Article 52(3) of the EU Charter, when rights in the EU Charter correspond to rights in the ECHR, their meaning and scope are the same as those laid out by the ECHR and must be interpreted in the same way as the interpretation provided by the ECtHR.

81 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] OJ L 201, art. 5.

82 Articles 5(1) of Directive 2002/58/EC impose on Member States internet-based communications services to respect strict confidentiality requirements. Article 3 of Regulation 2021/1232 provides that these provisions of the Directive shall not apply to the confidentiality of communications involving the processing by providers of personal and other data in connection with the provision of number-independent interpersonal communications services provided that specific conditions outlined in the same article are fulfilled. The aim of the derogation is to enable tech companies to continue detecting and removing child sexual abuse material online on a voluntary basis.

To address this challenge, the EU adopted the Regulation 2021/1232<sup>83</sup> (hereafter “**the Interim Regulation**”) in 2021, which introduces temporary and limited rules derogating to the e-Privacy Directive for the purpose of combating online child sexual abuse, in recognition of Article 24(2) of the EU Charter (best interests of the child, see below)<sup>84</sup>.

The Interim Regulation aims to safeguard the **rights and freedoms of others**, namely the rights of children to protection from exploitation and abuse<sup>85</sup>, human dignity<sup>86</sup>, integrity of the person<sup>87</sup>, the prohibition of inhuman or degrading treatment<sup>88</sup>, the rights to general protection and care<sup>89</sup> and the right to private life and data protection of the children depicted in the CSAM in which they appear. It does so by allowing internet service providers to process personal and other data to the extent necessary to detect online child sexual abuse on their services and report it and to remove CSAM of their services on a voluntary basis<sup>90</sup>. In essence, this Interim Regulation allows for a period of three years for the continuing of **voluntary detection** of CSAM by internet service providers in the interest of protecting children from OCSE.

### 4.3 The Protection of Children from OCSE

At the EU level, the right of children to be protected from OCSE is not explicitly provided under the **EU Charter**, but it can be inferred from several other rights under the EU Charter. The protection of children from OCSE triggers the rights under:

- Article 1 on the protection of human dignity;

- Article 3 on the protection of the integrity of the person;
- Article 4 on the prohibition of inhuman or degrading treatment; as well as
- Article 24 on the rights of children to have the protection and care necessary for their well-being, and for which the child’s best interests must be a primary consideration<sup>91</sup>.

Article 24(2) of the EU Charter establishes that the **child’s best interests must be a primary consideration**, in all actions relating to children. It is in line with the United Nations Convention on the Rights of the Child (UNCRC), which enshrines the requirement of the best interests of the child as primary consideration in all actions concerning children. While the EU is not bound by the UNCRC, it is ratified by all 27 EU Member States and therefore, it is binding upon them. Under the UNCRC, States should ‘*ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration*’<sup>92</sup>.

The **CJEU** has acknowledged that **OCSE involves severe breaches of children’s fundamental rights**, particularly the right to protection of private and family life, individual physical and mental integrity, and the prohibition of torture and inhuman or degrading treatment<sup>93</sup>. The Court observes that for online crimes, collecting data like IP addresses may be essential for identifying the perpetrators, which necessitates specific laws to balance the rights and interests at stake. Governments have highlighted that this is particularly relevant for serious cases like child sexual abuse material, where such data is crucial for investigating and addressing offences<sup>94</sup>.

83 Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

84 Regulation (EU) 2021/1232, recitals 4, 5. In March 2024, the LIBE Committee endorsed a provisional agreement on the extension of the Interim Regulation until 3 August 2026, while interinstitutional negotiations are still ongoing for the Proposed CSA Regulation.

85 UNCRC, art. 19, 34.

86 EU Charter, art 1.

87 EU Charter, art 3.

88 EU Charter, art 4.

89 EU Charter, art 24.

90 Regulation 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-dependant interpersonal communication services for the processing of personal and other data for the purpose of combating online child sexual abuse [2020] L 274/41, art. 3.

91 EU Charter, art. 24. (1) Children shall have the right to such protection and care as is necessary for their well-being. (2) In all actions relating to children, whether taken by public authorities or private institutions, the child’s best interests must be a primary consideration. (3) [...]

92 Committee on the Rights of the Child (2021). [General comment No. 25 \(2021\) on children’s rights in relation to the digital environment](#).

93 CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020, pt. 126.

94 CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020, pt.154.

**“The European Court of Human Rights has held that the positive obligations flowing from Articles 3 and 8 of the ECHR, whose corresponding safeguards are set out in Articles 4 and 7 of the Charter, require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person through effective investigation and prosecution, that obligation being all the more important when a child’s physical and moral well-being is at risk”<sup>95</sup>.**

CJEU, *La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020.



**EU Directive 2011/93/EU (the CSA Directive)** on combating the sexual abuse and sexual exploitation of children reflects this obligation as well. Under

this Directive, acquiring or possessing, knowingly obtaining access via the use of ICTs, distributing, disseminating or transmitting, offering, supplying or making available, and producing child sexual abuse material are punishable as criminal offences<sup>96</sup>. The solicitation for sexual purposes (grooming) by adults of children under the age of consent by means of ICTs is also criminally punishable<sup>97</sup>. The CSA Directive harmonises the child sexual abuse offence definitions, including those applicable to the online environment, within the EU and obliges EU Member States to adopt preventive measures and to protect victims<sup>98</sup>. The CSA Directive refers to Article 24 of the Charter and the best interests of the child as justification for tackling the sexual abuse and exploitation of children.

To be noted that a recent Proposal<sup>99</sup>, published by the European Commission in February 2024, aims to recast the CSA Directive to enhance the fight against online child sexual abuse, given its increasing prevalence and recent technological development such as the use of AI to commit child sexual abuse.

<sup>95</sup> CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020, pt 128.

<sup>96</sup> United Nations. (1989). Convention on the Rights of the Child, art. 34 (here after “UNCRC”); UNCRC General Comment No. 13, para 25.

<sup>97</sup> Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335/17, art. 6.

<sup>98</sup> Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335/17, art. 6.

<sup>99</sup> Proposal directive 2024/0035 (COD) of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council framework decision 2004/68/JHA.

# 5. Striking a Balance



## KEY FINDINGS

According to the EU Charter, limitation to a right may be imposed under **four key criteria**: 1. Being provided by law; 2. Respect the essence of the right; 3. For the purpose of general interest; 4. Be proportional.

1

**Criterion 1. Lawful:** The law must clearly outline the extent to which the right to privacy will be limited, as well as the exact procedures, making it understandable and foreseeable for the average person. The Proposed CSA Regulation fulfils this requirement.

2

**Criterion 2. Essence of the right at stake:** The essence of the right to privacy may be respected if the interference does not allow for a “full overview” of an individual’s private life, through granting general access to personal data other than to what is strictly necessary to detect CSAM. The adoption of a legal framework such as the Proposed CSA Regulation is crucial to meet this requirement and ensure data minimisation and oversight.

3

**Criterion 3. Purpose of general interest:** The detection of CSAM helps identify and rescue children from OCSE and genuinely meets the objective of combating serious crime and safeguarding public security, which is a general interest of the EU. The Proposed CSA Regulation thus fulfils this criterion.

4

**Criterion 4. Proportional:** the proportionality test requires that the interference is appropriate, necessary and *stricto sensu* proportional. The measures proposed by the CSAM Regulation are deemed **appropriate** due to detection being the only suitable manner to combat CSM at scale, **necessary** due to the lack of other equally appropriate and less restrictive measures, **proportional stricto sensu**, as it aims to achieve the key fundamental value of protecting children against harm in a proportionate manner. The Proposed CSA Regulation would meet this requirement.



**“We do not think that there is a debate between online safety and privacy. Both of them are important and should be protected. Privacy is important, but when we talk about criminal acts or prevention of [criminal acts], it should be considered as less important. If you agree to use a certain platform, you should accept that online safety is more important than privacy”.**

(VOICE research, Child from Bulgaria)

Building upon the European legal framework of the right to privacy and as a preamble to the following analysis, it is imperative to underscore that **CSAM and grooming fundamentally violate the rights of the individuals depicted in the images and videos shared online, in addition to being a criminal offence.** The right to respect for private life is highly relevant for children, especially for those who have been victims of online sexual abuse. Effectively prioritising and safeguarding the privacy rights of victims and survivors is imperative in addressing this issue and ensuring a comprehensive legal response.

In addition, online features aiming at increasing privacy online (e.g. such as protecting when and how personal data is shared) serve as protecting factors against OCSE and are part of child safety by design approaches<sup>100</sup>. Therefore, **privacy and online child safety should be understood as complementary to each other.** Lastly, while seeking the use of technology to tackle the issue, privacy preserving tools should always be preferred.

The Proposed CSA Regulation raises concerns about potential impact on users' right to privacy. The EU Commission acknowledges that *“the measures contained in the proposal affect, in the first place, the exercise of the fundamental rights of the users of the services at issue”*, including the protection of personal data and right to privacy<sup>101</sup>.

Article 52(2) of the EU Charter provides the reference for evaluating measures restricting the exercise of the right to private life enshrined in Article 7 of the **EU Charter**<sup>102</sup>. To be justified, a limitation to the right to the respect of private life under Article 7 of the EU Charter must:

1. Be **provided for by law** in a way that is understandable and foreseeable for an average person;
2. **Respect the essence of the right concerned;**
3. **Genuinely meet the objective of general interest** recognised by the Union or the need to protect the rights and freedoms of others;
4. **Respect the principle of proportionality**<sup>103</sup>.

The subsequent analysis delves into a detailed examination of the above criteria required for justifying interference with the right to privacy under Article 7 of the EU Charter. Before delving into this analysis, it should be acknowledged that neither the CJEU nor the ECtHR have examined measures similar to those outlined in the Proposal. As a result, there exists a degree of inherent uncertainty, particularly in complex and sensitive matters such as the present ones. Definitive conclusions regarding the lawfulness or not of the interference of the Proposal with the right to the respect of private life under Article 7 EU Charter cannot be drawn.

<sup>100</sup> Terre des Hommes (2024). [Child Safety by Design Factsheet](#).

<sup>101</sup> Explanatory Memorandum to the Proposed CSAM Regulation (n 100) 12.

<sup>102</sup> However, it is also important to consider the criteria outlined in Article 8(2) ECHR, as interpreted by the ECtHR case law. Accordingly, any limitation to a right must be: lawful; necessary in a democratic society; in the interest of, among others, the prevention of a crime, or the protection of the rights and freedoms of others.

<sup>103</sup> EU Charter, art. 52(1).



## 5.1 Provided for by Law

Under EU law, limitations to fundamental rights must be provided for by law<sup>104</sup>. The requirements of legality outlined in Article 52 pertain to both the **existence of the law** itself and the **specific qualities that this legislation must possess**. This section analyses if and how the Proposed CSA Regulation fulfils both of the requirements.

According to the ECtHR and the CJEU case-law<sup>105</sup>, legislation that allows interference with a right must clearly define the extent of that limitation. This means more than just having a legal basis; it must also precisely outline the **scope** of the interference. The legislation must be **accessible, foreseeable** and allow for effective **judicial oversight**. It can be flexible to accommodate different scenarios and evolving circumstances<sup>106, 107</sup>.

In the context of police surveillance, the ECtHR has held that the law must be sufficiently **clear** in its terms to give citizens an adequate indication of the **conditions and circumstances** in which authorities are empowered to resort to “any measures of secret surveillance and data collection”<sup>108</sup>. In addition, the ECtHR also emphasised the importance of the existence of an **independent oversight** if an interference with the right to private life is to be permitted<sup>109</sup>.

On interferences with the rights guaranteed by Articles 7 of the Charter, the CJEU has added that it is necessary that the EU legislation “lay down clear and precise rules governing the scope and application of a measure and **imposing minimum safeguards**, so that the persons whose personal data is concerned

*have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data”*<sup>110</sup>.

The Proposed CSA Regulation clearly sets out the circumstances when a user’s communication may be scanned, the exact procedure and steps to be followed for the issuance of a detection order, as well as the safeguards needed, time-limits on the duration of the detection orders, and the procedures and modalities for supervision by the EU Centre and the independent administrative authorities. Through supervisory and judicial oversight and avenues for redress, it also assures this process includes the involvement of judicial authority and due process<sup>111</sup>. It is also important to note that decisions regarding the opening of investigations or prosecutions are made through a human, individualised evaluation of the situation. These situations are not made by the service providers but by competent law enforcement authorities, in accordance with the applicable law. As the European Commission recalls, “no decision is taken based on the result of the hit/no-hit automated detection carried out and the subsequent report by the service provider”<sup>112</sup>. In fact, this reporting process is subject to a specific requirement set out in Articles 12 and 13 of the Proposed Regulation and will undergo verification by the EU Centre, guaranteeing that reports to law enforcement are not manifestly unfounded<sup>113</sup>.

These safeguards ensure that there is a clear limit on the interference with the right to privacy. Therefore, we can conclude that **the Proposed CSA Regulation fulfils the first requirement** of Article 52(1) of the EU Charter.

104 EU Charter, art. 52(1).

105 ECtHR, *Big Brother Watch and Others v United Kingdom*, 25 May 2021, pt. 333, and the case law cited. See, among others, CJEU, C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, 16 July 2020.

106 CJEU, C-817/19, *Ligue des droits humains ASBL v Conseil des Ministres*, 21 July 2022, pt. 114.

107 CJEU, C-401/19, *Poland v Parliament and Council*, 3 June 2022, pt. 74.

108 ECtHR, *Shimovolos v Russia*, 21 June 2011, pt. 68.

109 ECtHR, *Big Brother Watch and Others v United Kingdom*, 25 May 2021, pt. 365.

110 CJEU, C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, pt. 91.

111 ECtHR, *Petra v Romania*, 24 September 1998, pt. 37.

112 Comments of the services of the Commission on some elements of the Draft Final Complementary impact assessment of the Commission proposal for a regulation laying down rules to prevent and combat child sexual abuse, presented by ECORYS, at the request of the European Parliament’s Committee on Civil liberties, justice and home affairs (LIBE), p. 10.

113 Proposed CSA Regulation, art. 48.

## 5.2 Respecting the Essence of the Right Concerned

If a restriction on the exercise of fundamental rights undermines the **core essence of those rights**, the measures would inherently contravene the Charter, regardless of any assessment of proportionality. To our knowledge, there is no case law where the judges of the CJEU have provided a positively formulated general and abstract definition of respecting the essence of the right concerned.

In its case *Schrems*, the CJEU has ruled that *“legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter”*<sup>114</sup>.

In *Digital Rights Ireland*, the CJEU acknowledges a significant intrusion upon the right to private life posed by Directive 2006/24/EC<sup>115</sup>, mandating internet service providers to retain telecommunications data for crime prevention and prosecution. However, the Court concluded that this directive did not violate the essence of the right to private life, given that *“the directive does not permit the acquisition of knowledge of the content of the electronic communications as such”*<sup>116</sup>. In the same line, in the *La Ligue des droits humains* case, the CJEU considered that measures potentially revealing specific personal information **did not undermine the essence of the fundamental rights involved**, meaningly Articles 7 and 8 of the EU Charter, due to the fact that the information in question **did not allow for a “full overview” of individual’s private life**<sup>117</sup>.

Both precedents are relevant and based on this case law, it cannot be inferred that the Proposed CSA Regulation grants general access to content data or a full overview of individuals’ private lives, as the

proposed regulation restricts detection to criminal content exclusively. As we exposed in section 3, the detection technology is explicitly engineered to identify CSAM and merely identifies grooming patterns associated with such content. It does not interpret or understand content. Privacy preserving technologies also minimise the amount of data processed and/ or pseudonymise or anonymise the information to further ensure privacy. Because CSAM detection technologies solely assess the presence of CSAM, based on hashes or machine learning algorithms, they do not provide a full overview of individuals’ private lives.

The adoption of a regulatory framework that can have an oversight on how those technologies are deployed and whether they sufficiently meet data minimisation standards is crucial to meet this requirement.

Another consideration in assessing whether or not the Proposed CSA Regulation would amount to access on a generalised basis to the content of electronic communications is the fact that the measures under the Regulation are only target at specific services which have proven to present significant risk of online child sexual abuse despite the implementation of mitigation measures. In addition, the detection measure would only arise from a Court order based on an implementation plan that would lay down the guarantees for minimising any interference with the right to privacy to what is strictly necessary to detect and remove OCSE. Lastly, under the Proposed CSA Regulation, the detection orders are limited in time and subject to continuous oversight.

In conclusion, the proposed measures under the Regulation do not in any way provide access to the content of electronic communications on a general basis, nor provide for a full overview of the private life of users. It should therefore be considered that **the essence of Article 7 EU Charter is not compromised by the Proposed CSA Regulation**.

<sup>114</sup> CJEU, C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, pt. 94.

<sup>115</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

<sup>116</sup> CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others*, 8 April 2014, pt. 39.

<sup>117</sup> CJEU, C-817/19, *Ligue des droits humains ASBL v Conseil des Ministres*, 21 July 2022, pt. 120.



### 5.3 Objective of General Interest

Article 52 of the EU Charter provides that limitations to a right can be made if they “*genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*”.

The notion of **general interest objective recognised by the EU** is very broad in scope, knowing that all objectives recognised by the EU are covered<sup>118</sup>. In *La Quadrature du Net*<sup>119</sup>, the CJEU identified three related categories of public interest objectives that can justify data retention by services providers: 1. Combating serious crime; 2. Safeguarding national security; 3. Prevention of serious threats to public security.

The objective of **combating serious crime** includes

the prevention, investigation, detection and prosecutions of criminal offences. Such objective can justify an interference with the right to private life and data protection, both enshrined in Article 7 and 8 of the EU Charter<sup>120</sup>. For instance, the CJEU recognised that the retention of data for the purpose of their possible transmission to the competent national authorities satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security<sup>121</sup>.

In *La Quadrature du Net* case, the CJEU has established that the objective of combating serious crime, in this case terrorist activities, can justify the general and indiscriminate retention of certain type of data if it meets specific requirements and safeguards such as being limited in time, the availability of effective judicial review and substantive safeguards against risks of abuse.

The CJEU affirmed that Article 52 of the Charter does not preclude legislative measures that, for the purposes of safeguarding national security, require electronic communications service providers to retain, generally and indiscriminately, traffic and location data, IP addresses assigned to the source of an Internet connection, data relating to the civil identity of users, “*where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists*”.

The measures are deemed compliant with EU law “*provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse*”.

CJEU, *La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020.

118 S. Peers & S. Prechal, ‘Article 52 – Scope and Interpretation of Rights and Principles’, in: S. Peers, *The EU Charter of fundamental rights: a commentary*, Oxford: Hart Publishing 2014, p. 1475.

119 CJEU, *Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020.

120 CJEU, *Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016, pt. 100.

121 CJEU, *joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others*, 8th April 2014, pt. 44.

In its case law, the CJEU has explicitly listed “the sexual exploitation of children” as offences that are inherently and indisputably extremely serious. The Court specifically ruled that an IP address assigned to the source of an internet connection without other data or metadata may be retained for combating serious offences such as online child sexual abuse material<sup>122</sup>.

This approach is consistent with ECtHR case law, which the CJEU will take into consideration in its assessment<sup>123</sup>. In *Trabajo Rueda v. Spain*, the ECtHR found that the searching of a personal computer by the police after a technician had found CSAM on it and informed the authorities pursued the legitimate aim of ‘crime prevention’. The Court emphasised the importance of **State protection for victims of OCSE**<sup>124</sup>.

Moreover, the ECtHR stated in its recent *Podchasov v. Russia* case law that while confidentiality of communications and **E2EE** are essential elements for preserving the right to respect for private life, **such a guarantee cannot be absolute** and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others<sup>125</sup>. In the case, the ECtHR found a violation of the right to the respect for private life under Article 8 ECHR because the legislation allowed public authorities to access the content of users’ electronic communications on a generalised basis and without **sufficient safeguards**<sup>126</sup>.

Necessary safeguards would include “clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity

and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness”, as mentioned by the ECtHR in the same case.

The purpose of detection orders outlined in the Proposed CSA Regulation is to fight against OCSE by detecting and removing CSAM online as well as detecting and investigating online child grooming<sup>127</sup>. This objective aligns with the broader goal of **crime prevention and prosecution of crime**. By addressing grooming instances and eliminating CSAM distribution, the regulation serves to protect these rights and mitigate the ongoing harm experienced by the depicted children.

Another point should be taken into consideration when identifying a legitimate objective pursued by the Proposed Regulation. EU law already **authorises** interpersonal communication service providers to implement **cybersecurity measures, including the use of detection tools**, to actively safeguard their services from threats, such as malware and phishing emails<sup>128</sup>. While ensuring the safety and efficiency of telecommunications services is a valid and important objective of general interest, the lack of a comparable level of intrusion into personal data for the more critical public interest of combating the dissemination of CSAM raises questions. CSAM detection tools operate in many ways similar to cybersecurity detection tools, aim to tackle a particularly serious crime and should therefore be considered as pursuing the objective of general interest of protecting children from OCSE.

The interference as laid out in **the proposed CSA Regulation can thus be considered as meeting the criterion of general interest** and protecting the right of children to be protected from OCSE.

122 CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020 pt 154.

123 According to Article 52(3) of the EU Charter, when rights in the EU Charter correspond to rights in the ECHR, their meaning and scope are the same as those laid out by the ECHR and must be interpreted in the same way as the interpretation provided by the ECtHR.

124 ECtHR, *Trabajo Rueda v Spain*, 30 May 2017.

125 ECtHR, *Podchasov v Russia*, 13 February 2024, pt. 65 and cited case law.

126 ECtHR, *Podchasov v Russia*, 13 February 2024, pt. 80 and 81.

127 Commission, ‘Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse: Explanatory Memorandum’ (Explanatory Memorandum to the Proposed CSA Regulation) 7.

128 Art. 40, Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).

## 5.4 Respect the Principle of Proportionality

Given the **absence of hierarchy between fundamental rights**, it is necessary, in the event of conflict, to “allow a fair balance to be struck between the various fundamental rights protected by the Community legal order”<sup>129</sup>. This refers to the principle of proportionality, which holds three substantive requirements:

1. **Appropriateness** of the measures taken;
2. The **necessity** of the measure; and
3. Proportionality **stricto sensu** of the measures.

### A. Appropriateness of the measures

Firstly, the measure must be appropriate to achieve the objective that is pursued, that is to say it must be at least **capable of contributing to its achievement**<sup>130</sup>. According to the CJEU jurisprudence, the principle of proportionality test requires that measures be appropriate for attaining the legitimate objectives pursued by the legislation but also that it does not go beyond the limits of what is appropriate and necessary in order to achieve those objectives<sup>131</sup>.

The review of compliance with the principle of appropriateness must be done depending on a number of factors, including, in particular, the issue at stake, the nature of the right at issue, the nature and seriousness of the interference and the object pursued by the interference<sup>132</sup>.

For instance, the CJEU has considered appropriate limitations on the exercise of the right to freedom of expression and information of users of online content-sharing services as a result of the use of automatic recognition and filtering systems detecting and blocking unlawful content for the purpose of

protecting intellectual property rights. The measure was deemed appropriate to reach the “legitimate objectives pursued or the need to protect the rights and freedoms of others”, considering that the measure is the least onerous and the disadvantages caused by it are not disproportionate<sup>133</sup>.

Regarding interference to the right to privacy, the CJEU has considered that the nature of the rights to protection of personal data and respect for private life requires to limit the discretion of the EU legislature to allow for interference, depending on the extent and seriousness of the interference. The Court, however, has ruled as appropriate the retention of data for pursuing the objective of investigating, detecting and prosecuting serious crime. A key consideration in this assessment was the growing importance of electronic communication and data retention as a valuable tool for criminal investigations<sup>134</sup>.

Regarding the appropriateness of the Proposed CSA Regulation for achieving the objectives pursued, it should be recalled that the European Commission conducted several impact assessments examining and comparing several policy alternatives in relation to the aim of combating OCSE<sup>135</sup>. The approved and final impact assessment showed that detection of online child sexual abuse is **suitable to achieve the aim of effectively tackling the serious criminal offenses** at stake, by protecting the fundamental rights of children. More specifically, the detection of known CSAM helps to prevent the re-victimisation of children, while the detection of unknown CSAM and grooming actually helps rescuing children from ongoing or imminent abuse<sup>136</sup>, as well removing illegal content from online platforms<sup>137</sup>.

Detecting and removing CSAM also pursues an objective of **crime prevention**. Recent research has shown that the easy access to CSAM leads to

129 CJUE, C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, 29 January 2008, pt. 68.

130 Opinion of Advocate General Saugmandsgaard Øe, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 19 July 2016, pt. 176.

131 For instance, CJEU. Case C-58/08. *Vodafone and Others*. 9 November 2010, para 74.

132 CJEU, *Digital Rights Ireland and Seitlinger and Others*, joined Cases C-293/12 and C-594/12 (GC), 8 April 2014, para 47.

133 CJEU, C-401/19, *Poland v Parliament and Council*, 26 April 2022, pt. 65.

134 Ibid, para 49.

135 CJEU, C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* 16 July 2020, pt. 176.

136 UK Government, *End-to-end encryption and child safety*, 2023. According to the National Crime Agency, the information that social media companies give to UK law enforcement contributes to over 800 arrests of suspected child sex offenders, and results in an estimated 1,200 children being safeguarded from child sexual abuse on average every month.

137 European Commission, Comments of the services of the Commission on some elements of the Draft Final Complementary Impact Assessment on the Commission Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, presented by ECORYS, at the request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) (here after “European Commission non-paper”), Ref. Ares(2023)3982785, 8 June 2023, p. 8.

addiction from viewers, who will further seek to commit in-person child sexual abuse<sup>138</sup>. In addition, CSAM websites use pyramid schemes to entice offenders to produce or obtain new content to gain access to libraries of CSAM, and therefore encouraging CSAM viewers to commit online and/or in person child sexual abuse to obtain such new material<sup>139</sup>.

The European Commission impact assessment also showed that **automated scanning is the only way to sufficiently detect CSAM at scale**<sup>140</sup>, which can be substantiated by the previously mentioned study led by Pfefferkorn (2022), where a consensus among service providers emerged, indicating that automated content scanning is considered the most effective method for detecting CSAM<sup>141</sup>.

Therefore, the measures under **the Proposed regulation can be considered appropriate** for achieving the objectives pursued.

## B. Necessity of the measures

The measure must be **necessary** for the pursuit of the said objective, which can only be the case in the **absence of any other measure** which would be equally appropriate while being less restrictive<sup>142</sup>. This condition also requires that the means implemented to achieve the objective **do not go beyond what is necessary to achieve it**<sup>143</sup>.

Two other types of measures deserve to be analysed here as complementary approaches to mandatory

detection: 1) **the voluntary detection** of CSAM and 2) **the public reporting** of CSAM.

The **voluntary detection of CSAM** has been in place for over a decade. In the face of regulatory inaction, some online platforms took upon themselves to detect and remove known and unknown CSAM, along with various serious online harms. The voluntary detection of CSAM has enabled US-based companies to report 105.6 million CSAM in 2023<sup>144</sup>. The drawback is that discrepancies exist to the extent those tools are used across the sector and gaps exist in the absence of legal requirements. The EC's impact assessment showed that voluntary actions have proven insufficient in preventing OCSE and providing victims with adequate assistance<sup>145</sup>. While mandatory detection efforts are crucial, recent legal analysis by Microsoft emphasises the significance of voluntary detection efforts in combating the dissemination of CSAM. By exclusively focusing on mandatory detection as proposed by the CSA Regulation, there is a risk that service providers may lack incentives to take proactive measures unless compelled by a detection order. This could result in less effective protection of children against OCSE. Failing to provide a legal basis for voluntary participation in detection could result in an increase in the dissemination of CSAM (due to the potentially more limited scope of the mandatory detection measures) and undermine efforts to combat it. In line with the conclusions of this legal analysis, we agree that mandating voluntary detection by service providers is a *"necessary complement to a regime based [solely] on detection orders"*<sup>146</sup>.

138 "ReDirection research demonstrates that searching for, viewing, and sharing CSAM is strongly correlated with seeking direct contact with children, as around 40% of respondents say that they have sought contact with a child after viewing CSAM. Additionally, nearly 60% of respondents say that they are afraid that their use of CSAM will lead to further sexual acts". Suojellaan Lapsia, Protect Children. ["Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry"](#) (2024).

139 Internet Watch Foundation, ["The Annual Report 2023: #BehindTheScreens"](#).

140 Explanatory Memorandum to the Proposed CSA Regulation (n 63) 14.

141 Pfefferkorn, R. (2022). Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers. *Journal of Online Trust and Safety*, 1(2).

142 Opinion of Advocate General Saugmandsgaard Øe, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others*, 19 July 2016, pt. 185.

143 CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, 9 November 2010, pt. 74.

144 NCMEC, [CyberTipline Report 2023](#), p. 10.

145 Explanatory Memorandum to the Proposed CSA Regulation (n 63) 9.

146 H. Graux and J. Clemens (Timelex), White paper on CSAM detection and prevention mechanisms under current and proposed European data protection regulation, 15 March 2023, p. 4.

While **public reporting of CSAM** contributes to the protection of children, including from ongoing abuse<sup>147</sup>, it also falls short in achieving the goal of fighting OCSE due to various barriers. These include the age of many victims, who are prepubescent and, as a result, may be too young to report. Additionally, some victims may face threats from offenders, dissuading them from reporting as well as the stigma and taboo associated with encountering such material acts, both deterrents to reporting. In 2023, only 265,542 reports came from public reporting of the total of 36,210,368 reports received by NCMEC<sup>148</sup>. Moreover, the data from the 2023 annual report of the IWF shows that proactive detection led to almost twice as many CSAM reports (257,375 reports), compared to public reporting (135,290 reports). The difference in numbers is staggering and demonstrates how public reporting is insufficient to meet the large volume of CSAM files in circulation.

This shows that **the same aim could not have been achieved by a less privacy-intrusive measure** and that therefore the measures set out by the Proposed Regulation are deemed **necessary** to reaching the objective of general interest of crime prevention and protection of the rights of children.

In assessing the necessity of using detection technology to find and report CSAM, both the online dimension and the fact the content itself is the crime must be taken into account. This was notably raised by the CJEU in *La quadrature du net* case law. There is an important difference between tackling online content that consists in a crime in and of itself and tackling online activities indicative of threats to national security that are carried out offline. This is not the case for OCSE, as the content is the crime itself.

In *La Quadrature du Net* case, the CJEU, when making the assessment of balancing rights, indicated that it is important to account of the fact that, *“where an offence is committed online, the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified”*. The assessment of necessity must account as to whether *“the detection of offences committed online may therefore prove impossible without recourse to a legislative measure”*. The CJEU confirmed that such scenario *“may occur, inter alia, in cases involving particularly serious child pornography offences, such as the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU”*.

CJEU, *La Quadrature du Net and Others v Premier Ministre and Others*, 6 October 2020, para 154.

Regarding the conditions that the measures must **not go beyond what is necessary** to achieve the objective of legitimate interest, the CJEU held that in order to satisfy this requirement, the legislation permitting the interference must lay down **“clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards [...] [and] it must, in particular, indicate in what circumstances and under which conditions**

*a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing”*<sup>149</sup>.

Following the European Commission non-paper<sup>150</sup>, the Proposed Regulation outlines precise guidelines for when a user's communication can undergo

147 Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, COM2023/797 final, 19 December 2023, p. 34.

148 NCMEC, [CyberTipline 2023](#).

149 CJEU, C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, 16 July 2020, pt. 176.

150 European Commission non-paper, p. 26.



scanning and incorporates multiple oversight mechanisms to prevent abuse of its provisions. It can be argued that the proposed rules are proportionate for the following reasons:

**1** **First**, the proposed Regulation does not entail a general and bulk scanning of communication on all online services. The Proposed CSA Regulation only applies to certain types of online services which have been found to be vulnerable to being misused for the purpose of requesting and disseminating CSAM and/or for the solicitation of children<sup>151</sup>. Moreover, the scope of the Regulation's provisions is **limited to what is strictly necessary** to obtain its objectives<sup>152</sup>, and **detection orders must be targeted and specified** by, where possible, limiting the detection to an identifiable part or component of the service or to specific users or specific groups of users<sup>153</sup>.

**2** **Secondly**, the Regulation sets out **strong oversight mechanisms**, including requirements about the independence and powers of the national authorities issuing and overseeing the execution of orders and the creation of the EU Centre as an assistance and advisory body. The Coordinating Authorities, EU Centre and national authorities are all legally bound by the EU Charter<sup>154</sup>. Detection orders are only issued after a diligent and objective assessment finding a significant risk of the specific service being misused for OCSE purposes, and after a case-by-case determination on the likelihood and seriousness of any potential negative consequence for the parties affected<sup>155</sup>.

**3** **Thirdly**, as regards the issue of privacy, the Regulation includes safeguards ensuring that the technologies used for detection

purposes are the **least privacy-intrusive** and in accordance with state of the art in the industry<sup>156</sup>. In simpler terms, the detection technologies are prohibited from extracting any information beyond what is strictly essential for CSAM detection. Potential risks associated with false positives and inaccurate reporting to law enforcement will be effectively addressed through the establishment of the EU Centre. The EU Centre can furnish validated indicators of child sexual abuse, exclusively permitting their use in detection processes, thereby preventing unwarranted reports from reaching law enforcement. Serving as an intermediary, the EU Centre will act as a filter between content reported by providers and the material forwarded to law enforcement, consequently reducing the potential error rate. Furthermore, the EU Centre has the capability to automatically alert companies utilising detection tools in case of erroneous notifications. Subsequent to such notifications, companies are obligated to take corrective measures<sup>157</sup>.

Drawing from case law concerning the assessment of the necessity of a measure, the ECtHR ruled in *Weber and Saravia v. Germany*, that there was no breach of Article 8 with regards to the “*strategic monitoring*” policy enacted to identify and avert serious dangers facing the country as there were **adequate and effective guarantees against abuses of the State’s powers**, and therefore Germany was entitled to consider the privacy interferences to have been “*necessary in a democratic society*”<sup>158</sup>. In the case of the Proposed CSA Regulation, there exists the **right to effective redress** for both service providers and users affected by the measures taken to execute detection orders<sup>159</sup>. The right to redress includes the right to challenge the detection order before the courts of the Member State of the

151 Explanatory Memorandum to the Proposed CSA Regulation (n 63) 7.

152 Explanatory Memorandum to the Proposed CSA Regulation (n 63) 7.

153 Proposed CSA Regulation (n 5) recitals 23.

154 EU Charter, art. 51.

155 Proposed CSA Regulation (n 5) recitals 21-22.

156 Explanatory Memorandum to the Proposed CSA Regulation (n 63) 7.

157 Comments of the services of the Commission on some elements of the Draft Final Complementary impact assessment of the Commission proposal for a regulation laying down rules to prevent and combat child sexual abuse, presented by ECORYS, at the request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), p. 3.

158 ECtHR, *Weber and Saravia v Germany*, 29 June 2006, pt. 5 to 8 and 137.

159 Proposed CSA Regulation (n 5) art 9(1).

judicial authority which issued the detection order<sup>160</sup>. Therefore, and similar to the *Weber case law*, the privacy of interference introduced by the Proposed CSA Regulation must be considered as “*necessary in a democratic society*”.

In the recent case of *Podchasov v. Russia*, the ECtHR highlighted that Russian domestic law, which compelled service providers to decrypt E2EE communications, posed a risk of undermining the encryption for all users due to a lack of sufficient safeguards correctly protecting the right to private life under Article 8 ECHR. Consequently, the legislation was deemed disproportionate to the legitimate aims pursued, which was national security and a violation of Article 8 ECHR was found. This is not the case with the Proposed Regulation, as it provides various safeguards to protect the right to private life. As demonstrated by our analysis, the Proposed Regulation clearly indicates to what extent the right to private life may be limited and describes the involvement of judicial and supervisory oversight. Moreover, the Proposed CSA Regulation only allows to the extent that is necessary to identify CSAM en grooming patterns associated with it. These are clear safeguards against possible abuses of power. The notable contrast between the deficient safeguards in Russian domestic law and the robust provisions outlined in the Proposed Regulation leads us to the conclusion that the ECtHR would not find a violation of Article 8 ECHR, in the event of a case being brought before it.

In light of all these safeguards, it is clear that the Proposed CSA Regulation entails strict rules and oversight mechanisms to ensure that the adverse effects to the right to privacy of users, which could be caused by CSAM detection, are as limited as possible, while still achieving its objective of combating OCSE. The provisions within the Regulation would substantially diminish the infringement upon victims’ rights by promptly identifying and halting their ongoing abuse, thereby reducing the incidence of

OCSE and upholding children’s rights by preventing their victimisation. This aligns directly with the aim of safeguarding their rights to protection from exploitation and abuse, human dignity, integrity of the person, the prohibition of inhuman or degrading treatment, and the rights to general protection and care.

It can be concluded that the measures proposed by the **Proposed Regulation are necessary to achieve the objective** of protecting children against sexual abuse and exploitation.

### C. Proportionality *stricto sensu* of the measures

Lastly, the measure must be proportionate in the *stricto sensu*, to the pursuit of the objective pursued, which means that a measure “*which interferes with fundamental rights may be regarded as proportionate only if the disadvantages caused are not disproportionate to the aims pursued*”<sup>161</sup>.

The Advocate General Saugmandsgaard Øe in the case *Tele2 Sverige AB v Post- och Telestyrelsen* specifies that “*the requirement of proportionality stricto sensu implies weighing the advantages resulting from the measure in terms of the legitimate objective pursued against the disadvantages it causes in terms of the fundamental rights enshrined in a democratic society. This particular requirement therefore opens a **debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in***”<sup>162</sup>. To our knowledge, the CJEU does not have any case law on the assessment of this criterion in relation to serious crime and typically concentrates on the first two criteria.

Both rights are fundamental pillars of our society and reflect our commitment to protect the vulnerable

160 Proposed CSA Regulation (n 5) art 9(1).

161 Opinion of Advocate General Saugmandsgaard Øe, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och Telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 19 July 2016, pt. 247.

162 Opinion of Advocate General Saugmandsgaard Øe, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och Telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 19 July 2016, pt. 248.

while also respecting individual autonomy and dignity. We argue the interference with the right to online privacy is proportional as **it strives to uphold essential values**, mainly children's right to protection against harm, and are the only **effective way** to address the issue of child sexual abuse and exploitation at scale. Studies found that when asked which one to prioritise, 66,91% of the caregivers surveyed said that they find child protection from online sexual abuse more important<sup>163</sup>.

The Proposed Regulation sets out strict safeguards to minimise the impact on users' rights and aims to balance between their rights and those of children. This is demonstrated by the fact that:

- Online service providers are required to conduct a data protection impact assessment and seek the opinion of the competent data protection authority regarding their implementation plan<sup>164</sup>, while no child rights impact assessment is required nor encouraged;
- The Coordinating Authorities must ensure that the request of the service providers for detection orders are as targeted as possible. Ideally, these orders should only pertain to sub-components of the service, if the indication of a significant risk is limited to such sub-components and if technically feasible<sup>165</sup>;

- The final decision to issue a detection order rests with a judicial or independent administrative authority, which must carefully balance all fundamental rights involved<sup>166</sup>;
- Service providers have an obligation to report on their detection practices to the Coordinating Authorities<sup>167</sup>;
- Finally, redress is ensured for affected service providers and/or users<sup>168</sup>.

While aiming to achieve an equilibrium between the imperative to protect children from online sexual exploitation and the importance of upholding individuals' right to privacy online, we argue that the Proposed Regulation primary focus is on the impact of privacy of users, while processes and safeguards do not require similar assessment on the impact of the measures or absence of it on the right of privacy of child victims and the right of children to protection against sexual abuse and exploitation.

Ultimately, through these comprehensive safeguards and mechanisms, the Proposed Regulation can be considered meeting the requirement of proportionality *stricto sensu* in regards to the consideration of impact on the right to privacy of users.

<sup>163</sup> Eurochild, Ecpat International, Terre des Hommes Netherlands, (2024). Speaking Up for Change: children's and caregivers' voices for safer online experiences.

<sup>164</sup> Proposed CSA Regulation (n 5) art 7(3).

<sup>165</sup> Proposed CSA Regulation (n 5) recital 23.

<sup>166</sup> Proposed CSA Regulation (n 5) art 7(4).

<sup>167</sup> Proposed CSA Regulation (n 5) art 9(3).

<sup>168</sup> Proposed CSA Regulation (n 5) art 9(1).



# 6. Findings and Recommendations

The rapid advancement of technology and widespread internet access has introduced unprecedented speed and ease in accessing and sharing information, but at the same time it has also created significant challenges in protecting fundamental human rights. Children are now more than ever particularly vulnerable to OCSE due to new methods of offending that eliminate the need for physical proximity, and new encryption technologies which guarantee total privacy of communications<sup>169</sup>.

**All children have the right to be protected from online child sexual exploitation and abuse**, and States must ensure that internet service providers control and remove CSAM as soon as possible<sup>170</sup>. Safeguarding children from online sexual exploitation and abuse is of utmost importance for ensuring their well-being and a safe and secure environment for their healthy development.

This report concluded that the protection of children from OCSE would **validly justify a potential interference with the right to privacy under Article 7 EU Charter**, and therefore under Article 8 ECHR, caused by CSAM detection orders under the Proposed Regulation, as the limitation:

- ☒ Is provided for by law
- ☒ Respect the essence of the right
- ☒ Genuinely meet an objective of general interest recognised by the EU
- ☒ Respect the principle of proportionality

The report also finds that technology solutions allowing the detection and removal of child sexual abuse and exploitation in a privacy preserving manner do exist and can be deployed at scale. The system of risk assessment, mitigation and detection introduced by the Proposed CSA Regulation is crucial for upholding the rights of victims and for rescuing children from ongoing abuse. Therefore, only remains the need to issue policies that deploy such solutions within the framework of a law that will ensure the adequate safeguards and conditions for minimising the interference on the right to privacy while effectively achieving the protection of children.

However, while reports highlight the inefficiency of relying solely on detection through public reports or voluntary detection compared to automated detection methods<sup>171</sup>, **it is imperative to complement such measures with preventive actions focused on early interventions**. Indeed, platforms should prioritise Child Safety by Design while empowering children through relevant digital safety skills<sup>172</sup>. Throughout the studies, the lack of safety-by-design measures was commonly identified by children as an element contributing to a decreased feeling of safety online. Often children feel overwhelmed by safety settings that are not user-friendly and difficult to navigate<sup>173</sup>. Children themselves mention the importance of tools such as age-verification, parental-control technologies or child-friendly versions of existing apps, such as YouTube Kids<sup>174</sup>.

Although online platforms and social media are making efforts to address child safety, such as by implementing minimum age requirements<sup>175</sup>, they still

169 CRC Guidelines on the OPSC (n 3), para 2; United Nations, 'Child and Youth Safety Online' (United Nations).

170 UNCRC (n 2) arts 19, 34.

171 Pfefferkorn, R. (2022). Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers. *Journal of Online Trust and Safety*, 1(2); Explanatory Memorandum to the Proposed CSA Regulation (n 63) 9.

172 Down to Zero Alliance, 'Child safety by design that works against online sexual exploitation of children' (2022)

173 Eurochild, Ecpat International, Terre des Hommes Netherlands, (2024). Speaking Up for Change: children's and caregivers' voices for safer online experiences.

174 Ibid.

175 Down to Zero Alliance, 'Child safety by design that works against online sexual exploitation of children' (2022), 7.

lack a comprehensive and effective set of measures to prevent and detect OCSE<sup>176</sup>. Based upon the findings of this report and in order to strike the fairest balance possible between the need to address OSCE and the importance of respecting privacy rights online, it is recommended that the CSA regulation:

- Promotes a flexible system of detection by creating a **legal basis for voluntary detections** alongside the legal framework for automatic detection methods.
- Examines the technical characteristics and constraints of each platform in order to provide platform-specific mitigations.
- Puts forth the importance of **Child Safety by Design** in combating OSCE, including strong requirements for effective age verification and assurance.
- Promotes a **child rights risk assessment** approach alongside the already existing data protection impact assessment approach.



<sup>176</sup> Down to Zero Alliance, 'Child safety by design that works against online sexual exploitation of children' (2022), 7.

<sup>177</sup> ECPAT International, Eurochild & Terre des Hommes Netherlands. (2023). [Behind the screens: early findings from the VOICE research.](#)

<sup>178</sup> ECPAT International, Eurochild & Terre des Hommes Netherlands. (2024). [Speaking Up for Change: children's and caregivers' voices for safer online experiences.](#)

# ANNEX 1: GLOSSARY

<b>Automated Content Scanning</b>	Technology designed for the automated monitoring or scanning of users' communications.
<b>Child</b>	Any natural person below the age of 18 years.
<b>Child Safety by Design</b>	Child Safety by Design is an approach aimed at addressing online dangers by proactively anticipating potential harms and integrating protective measures into the design, development, and implementation of digital services and products with a view to mitigate or eliminate risks <sup>179</sup> .
<b>Child Sexual Abuse Material (CSAM)</b>	The term Child Sexual Abuse Material is used as an alternative to "child pornography" and refers to "material depicting acts of sexual abuse and/or focusing on the genitalia of the child". This can also include wholly or partly computer-generated CSAM <sup>180</sup> .
<b>End-to-end encryption (E2EE)</b>	End-to-end encrypted communications are systems encrypting messages in a way so that only the unique recipient of a message can decrypt it, thereby prevent third parties from accessing data while it is being transferred from sender to recipient <sup>181</sup> .
<b>EU Directive</b>	A legal act of the EU that sets specific objectives for EU member states to achieve <sup>182</sup> .
<b>EU Regulation</b>	An EU Regulation is a legal act by the EU which has general application, is legally binding in its entirety and is directly applicable in all EU Member States <sup>183</sup> .
<b>European Court of Human Rights</b>	An international court that hears cases related to violations of the European Convention on Human Rights.
<b>Grooming</b>	Online grooming, or online child solicitation, is " <i>a practice where an adult establishes/ builds a relationship and 'befriends' a child online to facilitate either their online or offline child sexual abuse</i> " <sup>184</sup> .
<b>Hash</b>	A 'hash' is a unique code, or string of text and numbers generated from the binary data of a picture <sup>185</sup> .
<b>Hashing</b>	Hashing is the process of assigning a unique hash value to an image/video using an algorithm so that hash technology can recognise duplicate and edited copies of the image/videos <sup>186</sup> .

179 Down to Zero Alliance (n 95).

180 S. Greijer and J. Doek, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT International 2016) (adopted by the Inter-Agency Working Group on Sexual Exploitation of Children, Luxembourg, 28 January 2016) (Luxembourg Guidelines) 35-38.

181 A. Greenberg, 'Hacker Lexicon: What Is End-to-End Encryption?' (Wired, 25 November 2014)

182 Art. 288, The Treaty on the Functioning of the European Union (TFEU), Official Journal of the European Union, C 326, Volume 55, 26 October 2012.

183 Art. 288, The Treaty on the Functioning of the European Union (TFEU), Official Journal of the European Union, C 326, Volume 55, 26 October 2012.

184 S. Greijer and J. Doek, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT International 2016) (adopted by the Inter-Agency Working Group on Sexual Exploitation of Children, Luxembourg, 28 January 2016) (Luxembourg Guidelines) 51.

185 IWF, [Annual report 2024 Glossary](#).

186 InHope, 'What is image hashing?' (Inhope)

<b>Information and Communication Technologies</b>	Information and communication technologies (ICTs) are a set of technological tools and resources used to transmit, store, create, share or exchange information. Examples are the Internet, broadcasting technologies and telephony <sup>187</sup> .
<b>Online Child Sexual Abuse</b>	The online dissemination of child sexual abuse material and the solicitation of children <sup>188</sup> .
<b>Online Child Sexual Exploitation</b>	Online child sexual exploitation “ <i>includes all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment</i> ” <sup>189</sup> .
<b>Online Privacy</b>	Online privacy is the ability to control one’s own identity and personal information in the online environment <sup>190</sup> . This also includes control over one’s own online correspondence.

187 Food and Agriculture Organisation of the United Nations, 'Information and Communication Technologies (ICT)' (FAO).

188 Proposed CSA Regulation (n 5) art 2.

189 S. Greijer and J. Doek, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT International 2016) (adopted by the Inter-Agency Working Group on Sexual Exploitation of Children, Luxembourg, 28 January 2016) (Luxembourg Guidelines) 24.

190 Winston & Strawn LLP, 'What is the Definition of Online Privacy?' (*Winston*)

# ANNEX 2: POTENTIAL VIABLE CSAM DETECTION TECHNOLOGIES

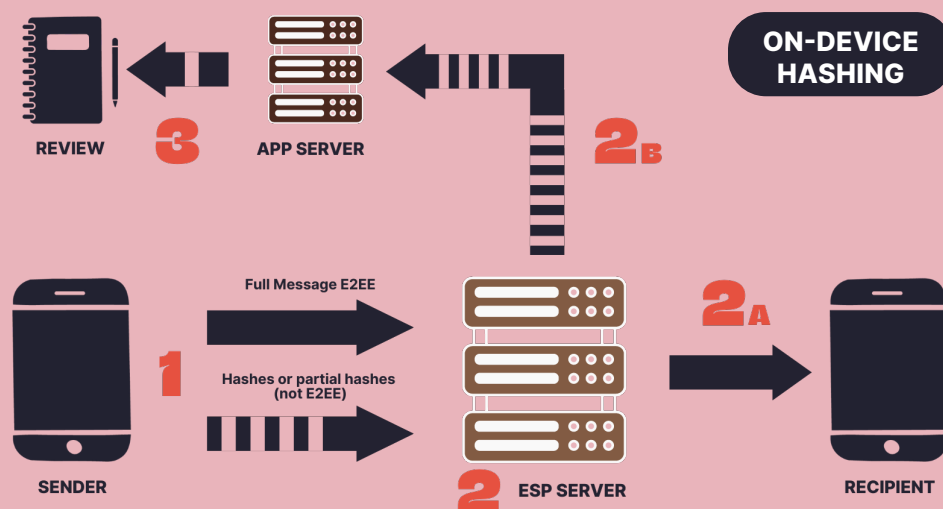
## Examples of potential CSAM detection technologies

### On-device hashing and matching

On-device hashing and matching can be done either fully on the device, or partially at the server. Through on-device full hashing with matching at the server, hashes are created of images and videos within communications (including E2EE) and then compared to a database of known CSAM hashes on the server<sup>191</sup>. Another possibility is on-device partial hashing with remaining hashing and matching at the server, which works in principle like on-device full hashing, only that in this case part of the hash is generated on the device, and the rest at the server<sup>192</sup>. These technologies can be used to detect known CSAM, but not new or heavily modified versions of known CSAM<sup>193</sup>.

PhotoDNA is a popular hash used to combat CSAM. It was originally developed by Microsoft and Dartmouth in partnership with NCMEC to help online service providers detect CSAM among the billions of images shared online<sup>194</sup>. PhotoDNA works by creating a unique signature, or hash, for a given image. It starts with an image identified as CSAM by trusted sources such as NCMEC and law enforcement. The image is transformed into a black and white format and resized uniformly. It is then divided into squares, each assigned a numerical value representing the unique shading within. These numerical values collectively form the hash for that image. Hash values for known CSAM can be compared to other images to identify copies, a process known as matching. This process is used to identify and flag harmful content online and filter out known CSAM from collections of images. The hash represents a unique digital identifier for each image, remaining consistent even if the image is altered<sup>195</sup>.

Figure 2. On-device hashing and matching



<sup>191</sup> Politico, 'Technical Solutions to Detect Child Sexual Abuse in End-to-end Encrypted Communications' (Politico.eu, September 2009).

<sup>192</sup> Politico, 'Technical Solutions to Detect Child Sexual Abuse in End-to-end Encrypted Communications' (Politico.eu, September 2009).

<sup>193</sup> Politico, 'Technical Solutions to Detect Child Sexual Abuse in End-to-end Encrypted Communications' (Politico.eu, September 2009).

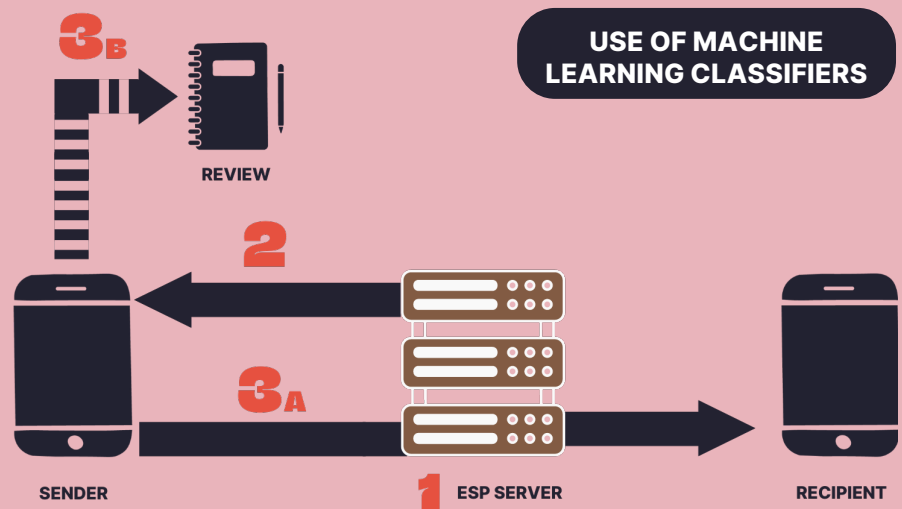
<sup>194</sup> Microsoft Digital Crimes Unit, [PhotoDNA](#).

<sup>195</sup> ECPAT Internet and Technology Factsheets, "What are hashes? What is PhotoDNA?". For further analysis, Martin Steinebach. 2023. [An Analysis of PhotoDNA](#). In *The 18th International Conference on Availability, Reliability and Security (ARES 2023)*, August 29--September 01, 2023, Benevento, Italy. ACM, New York, NY, USA

## On-device use of classifiers

With on-device use of classifiers, the servers produce classifiers, a set of characteristics determining if the content of a message or media are OCSE related, to identify OCSE<sup>196</sup>. These are produced and kept up to date using extensive labelled data of verified OCSE and non-OCSE to train the system<sup>197</sup>. These classifiers are sent to the sender's device which applies them to detect OCSE before encryption takes place<sup>198</sup>. This technology is able to detect both images and videos as well as instances of grooming<sup>199</sup>.

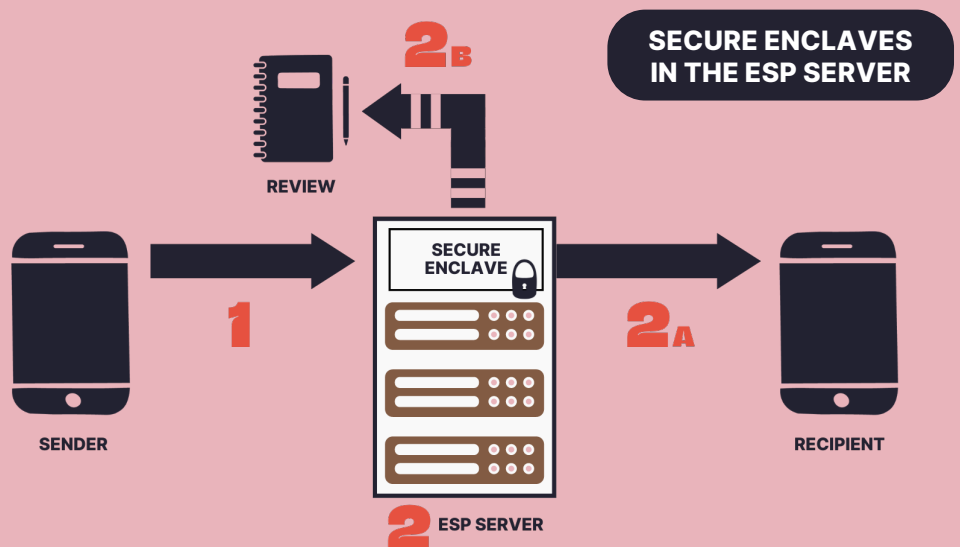
**Figure 3. On-device use of classifiers**



## Secure enclaves in the server

With the secure enclaves in the server system, the sender device sends the encrypted message to the enclave in the server, which allows compute intensive operations to happen in a closed environment in the cloud<sup>200</sup>. Here, the message is decrypted and a tool to detect CSAM is used<sup>201</sup>. This system can only be used to detect known CSAM<sup>202</sup>.

**Figure 4. Secure enclaves in the server**



<sup>196</sup> Politico, 'Technical Solutions to Detect Child Sexual Abuse in End-to-end Encrypted Communications' (Politico.eu, September 2009), 12.

<sup>197</sup> Ibid.

<sup>198</sup> Ibid.

<sup>199</sup> Ibid.

<sup>200</sup> Ibid., 14.

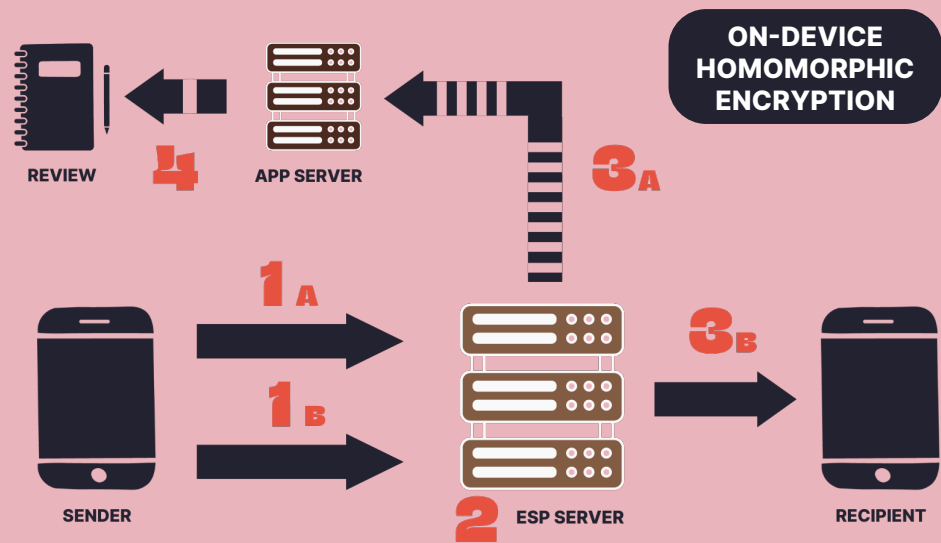
<sup>201</sup> Ibid.

<sup>202</sup> Ibid.

On-device homomorphic encryption with server-side hashing and matching

In on-device homomorphic encryption with server-side hashing and matching, the sender’s device sends to the server encrypted messages and images or videos homomorphically encrypted, meaning an encrypted version of the hash to be computed from the encrypted image<sup>203</sup>. The server extracts hashes from the homomorphically encrypted images or videos and compares the hash against a database of known CSAM<sup>204</sup>. This system can only be used to detect known CSAM<sup>205</sup>.

Figure 5. On-device homomorphic encryption with server-side hashing and matching



203 Ibid.  
204 Ibid.  
205 Ibid.