Routledge
Taylor & Francis Group

Victims & Offenders

An International Journal of Evidence-based Research, Policy, and Practice

ISSN: 1556-4886 (Print) 1556-4991 (Online) Journal homepage: www.tandfonline.com/journals/uvao20

Obligations of Online Service Providers to Fight Against Child Sexual Abuse Material—a Systematization of EU Law

Salomé Lannier

To cite this article: Salomé Lannier (2026) Obligations of Online Service Providers to Fight Against Child Sexual Abuse Material—a Systematization of EU Law, Victims & Offenders, 21:3, 506-534, DOI: 10.1080/15564886.2025.2557901

To link to this article: https://doi.org/10.1080/15564886.2025.2557901

Published online: 23 Mar 2026.

VICTIMS & OFFENDERS
2026, VOL. 21, NO. 3, 506–534
https://doi.org/10.1080/15564886.2025.2557901

Routledge
Taylor & Francis Group

Obligations of Online Service Providers to Fight Against Child Sexual Abuse Material—a Systematization of EU Law

Salomé Lannier

Department of Law, Faculty of Law, Economy and Finance, University of Luxembourg, Luxembourg, Luxembourg

ABSTRACT

This paper examines the obligations of online service providers (OSPs) in the European Union (EU) to prevent and combat child sexual abuse material (CSAM). Through textual analysis of key EU legal frameworks, including the *Digital Services Act* and the *Proposal for a Regulation laying down rules to prevent and combat child sexual abuse*, this study assesses the illegal materials and OSPs targeted by these texts, their core obligations, and enforcement mechanisms. Findings indicate complex, overlapping regulatory requirements across EU law, highlighting tensions between child protection, technological limitations, and potential overreach affecting freedom of expression.

KEYWORDS

Child sexual abuse material; online service providers; child pornography; grooming

Legislators increasingly intend to leverage technology to prevent and combat child sexual abuse material (CSAM), particularly by drafting new obligations to online service providers (OSPs). This paper aims to systematize these obligations under EU law.

CSAM represents an egregious violation of fundamental rights of children (Finkelhor et al., 2024; Gewirtz-Meydan et al., 2018; Paul et al., 2024), exacerbated by its availability and accessibility online. In 2022, the U.S. National Center for Missing and Exploited Children analyzed more than 32 million reports of CSAM received from across the globe and, from 2020 to 2022, the Internet Watch Foundation (IWF) reported a 360% increase of self-generated sexual materials of 7- to 10-year-olds (WeProtect Global Alliance, 2024). According to the IWF, in 2023, 51% of reports were traced to hosting services in EU countries (IWF, 2024a). Recent phenomena, such as "sharenting," meaning the sharing by parents of images of their children online, and the increased time spent online during COVID-19 lockdowns, have further compounded the spread of CSAM (Anillo et al., 2023; Salter et al., 2021; Ugwudike et al., 2024), as offenders adapt to technological advances and benefit from technical opportunities/affordances to evade detection such as anonymity or encryption (Bélair et al., 2024; Chopin & Décary-Hétu, 2023).

In response, the European Union (EU) has intensified efforts to combat CSAM from both a criminal and digital law perspective. Building upon foundational texts such as *Joint Action 97/154/JHA* of 1997, which targeted human trafficking and child exploitation under the Treaty

CONTACT Salomé Lannier salome.lannier@uni.lu Department of Law, Faculty of Law, Economy and Finance, University of Luxembourg, Weicker Building, 4 rue Alphonse Weicker, Luxembourg L-2721, Luxembourg

on EU, the EU has since introduced numerous policies addressing CSAM. Key milestones include the European Commission's report (European Commission, 2020, p. 14) and the 2022 *Strategy for a Better Internet for Kids* (European Commission, 2022). Particularly, the role of OSPs is currently under the scrutiny of public organizations, scholars, and nongovernmental organizations (NGOs) due to the debate around the European Commission's (2022) *Proposal for a Regulation laying down rules to prevent and combat child sexual abuse* (*CSAR Proposal*). As CSAM is predominantly disseminated through accessible and affordable online platforms (B. G. Westlake, 2020), OSPs increasingly play a critical role in international and national cyber strategies in identifying and reporting illegal content (Edwards et al., 2021; Holt et al., 2020; Quayle & Koukopoulos, 2019).

The technological landscape for detecting and combating CSAM has evolved significantly in recent years, with advances spearheaded by both private companies and academic institutions (Lee et al., 2020). A central component of CSAM detection technology involves algorithms that automate content scanning and hashing, meaning transforming an image into a numeric value, such as through Microsoft's PhotoDNA, which generates unique digital fingerprints of known CSAM and compares online content against these hashes (A. Krishna, 2021; Lee et al., 2020). Various detection methods are now employed to analyze online content—enabling the identification and removal of CSAM, including in newer forms of content such as video (B. Westlake et al., 2022), to tackle new forms of CSAM (Dushi, 2018, p. 21; Teunissen & Napier, 2023). Innovation has also supported the development of chatbots simulating child personas to identify potential offenders (Georgieva et al., 2019) as well as blocking and warning mechanisms, employed, for instance, by search engines or pornography websites, which help deter users from attempting to access CSAM by alerting them to the illegality of such searches (Henry, 2020; Prichard et al., 2022).

The unique role of OSPs in combating CSAM is underscored by the advantages inherent in their resources and technical capabilities (Holt et al., 2020). They have access to large data sets and advanced technologies that may exceed the resources available to traditional law enforcement authorities (LEAs). These capacities empower OSPs to respond to online criminal threats, including CSAM distribution, at a scale and speed that government agencies alone might not achieve (Holt et al., 2020). OSPs can also leverage contractual terms with users—such as Terms of Service—to regulate behavior and communicate their legal obligations to end users. Through these agreements, providers establish operational frameworks that include stipulations regarding information sharing with LEAs, ultimately contributing to the disruption of CSAM distribution channels (Broadhurst, 2019). As a result, many OSPs "are actively detecting and removing CSAM" (Teunissen & Napier, 2022, p. 9).

Yet, approaches and efforts to combat CSAM are inconsistent and fragmented among platforms (Gurriell, 2021). Research indicates that removal practices diverge based on motivation, legal framework, and the speed of action, prompting calls for standardized regulations that would legally obligate OSPs to adopt consistent CSAM prevention and removal strategies (Martellozzo & DeMarco, 2020; Maxwell et al., 2024). Consequently, the role of OSPs in fighting CSAM has grown increasingly complex, necessitating a detailed examination of their technological, legal, and procedural obligations under existing legal frameworks to identify gaps and overlaps.

Traditionally, legal reactions to criminal offenses have centered on criminal law enforcement: OSPs might qualify as offenders or accomplices for CSAM offenses. However, OSPs

benefit from restrictive criminal liability regimes, being usually liable only for content they have knowledge of (in the United Stated, *Section 230 U.S. Code*; in the European Union, *Digital Services Act* (*DSA*), Article 6). For instance, under the EU's *CSAR Proposal*, providers "shall not be liable for child sexual abuse offences solely because they carry out, in good faith," detection and prevention activities (Article 19). Differently, particularly to combat CSAM, national initiatives have developed self-regulatory or mandatory frameworks for cooperation among OSPs and LEAs. In the United States, the 2008 *Protect Our Children Act* (creating *18 U.S. Code Section 2258A*) has made it an obligation for OSPs to report CSAM to the National Center for Missing and Exploited Children (Bleakley et al., 2023; A. Krishna, 2021; Thakor et al., 2023). Conversely, the European Union has passed a fragmented framework to regulate technology (Graef and van der Sloot, 2024; Papakonstantinou and De Hert, 2024), including to prevent and combat CSAM. However, no research, to our knowledge, has systematized the diverse obligations of OSPs to fight against CSAM under EU law.

Therefore, this paper seeks to address the question, To what extent are OSPs in the European Union legally compelled to combat CSAM and how might these obligations overlap or complement one another across different legal frameworks? Through a systematic analysis of selected EU legal texts, we will examine the obligations imposed on OSPs, assessing the scope and enforcement measures involved. This analysis provides a framework to understand the European Union's regulatory approach to CSAM and highlights the unique position of OSPs within it. By analyzing transversally various EU frameworks, the paper underlines multiplied risks of overlaps and inconsistencies that might hamper the fight against CSAM. The paper will proceed by presenting the methodological approach, to be followed by an examination of the relevant legal obligations, focusing on the personal and material scope of these obligations—meaning which OSPs and illegal materials are targeted—and related enforcement measures.

Method

The method of this paper lies in the textual analysis of the law to systematize the main legal components of obligations of OSPs to fight against CSAM endorsed by selected EU law. The corpus of this study is made of six texts, including two proposals under negotiation (as in October 2024). The two proposals are analyzed as in the version published by the European Commission.

The role of OSPs was already mentioned back in the *Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography* (*Directive 2011/93/EU*), the first EU text to mandate Member States to criminalize what is still called child pornography (see section defining "sexual abuse material"). Member States had to transpose this directive in their national law by December 18, 2013 (Article 27.1 *Directive 2011/93/EU*).

Over the following years, OSPs faced increased obligations to identify and report online offenses, including child pornography. Firstly, an amendment to the *Audiovisual Media Services Directive* (*AMSD*, *Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services*) has introduced mention of child pornography by *Directive (EU) 2018/1808*. Member States had to transpose this new provision by September 19, 2020 (Article 2.1 *Directive (EU) 2018/1808*). Two years later, the *DSA* crafted

a general framework for OSPs' obligations in combatting online illegal content (*Regulation (EU) 2022/2065 on a Single Market For Digital Services*, *DSA*) (Husovec, 2024; Stringhi, 2024). Depending on the provisions, the text has been applicable since November 16, 2022 or February 17, 2024 (Articles 92 and 93 *DSA*).

In parallel, the EU legislators have taken an interest in proposing and adopting various texts dedicated to the obligations of OSPs to prevent and combat child pornography/CSAM. On July 14, 2021, the European Union adopted *Regulation (EU) 2021/123 on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service (NIICS) providers for the processing of personal and other data for the purpose of combatting child sexual abuse online*. It applied from 30 July 30, 2021, to 3 August 3, 2024 (Article 10) hence the text known as the *Interim Regulation*. In the meantime, the European Commission published the *CSAR Proposal* in 2022. Given that the text faces many criticisms (see Section Lex specialis: CSAM-specific frameworks), it was still under negotiation by the end of the applicable period of the *Interim Regulation*. Therefore, the applicability of the *Interim Regulation* was extended until April 3, 2026, by *Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024*. Finally, given that the terminology used under the *CSAR Proposal* did not match with *Directive 2011/93/EU*, the European Commission published in 2024 a *Proposal for a Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material*, which would replace the currently applicable directive (*Recast of Directive 2011/93/EU*).

To understand the scope and structure of this study, it is essential to clarify how the relevant EU legal instruments differ in nature and how they relate to one another. Firstly, a selection is made of both directives and regulations (see Table 1). The former are not, in principle, directly applicable. It means that they do not, by themselves, create obligation to private persons, such as OSPs. They only mandate States to adopt national provisions with detailed obligations (Article 288 *Treaty on the Functioning of the EU*) (Klamert & Loewenthal, 2019). Yet, the selected directives remain important to map out OSPs' obligations to combat CSAM, even when not directly applicable, as it guides the evolution of EU law. Nevertheless, this creates a limitation to this study, as it does not include national law in its scope, which can adopt more-stringent obligations for OSPs. Secondly, the interaction

Table 1. Selected EU law.

Title	Applicability
Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography	Transposition by December 18, 2013
Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services	Transposition by September 19, 2020
Regulation (EU) 2022/2065 on a Single Market For Digital Services	From 16 November 16, 2022, or February 17, 2024, depending on provisions
Regulation (EU) 2021/123 on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service (NIICS) providers for the processing of personal and other data for the purpose of combatting child sexual abuse online	From July 30, 2021, to April 3, 2026
Proposal for a Regulation laying down rules to prevent and combat child sexual abuse	Under negotiation
Proposal for a Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material	Under negotiation

among these texts must be clarified. Mainly, the *DSA* acts as the lex generalis, "a common set of rules regarding the obligations and responsibilities of the suppliers from the entire unique market, that the Commission wants to complete with specific provisions about child online sexual abuse" (Tolbaru, 2022, p. 350) (Article 2.4 *DSA*). Therefore, if the other texts set different or additional rules, they should be applied in priority, as lex specialis.

In analyzing these texts, this paper will focus on four key components based on the obligations identified in the legal framework (see Table 2). Firstly, the paper comments on the material scope of the texts, particularly in view of the European Commission's objective to modify EU law terminology from "child pornography" to CSAM. It is of utmost importance to clarify the type of illegal content targeted by the obligations, which will guide the OSPs in implementing those. Secondly, one must understand to which OSPs the selected obligations apply. Thirdly, the core element of the study is the obligations provided for in the texts. The conjunction of these three elements will shed light on the potential overlaps or gaps of the legislation. Fourthly, the paper will briefly assess the enforcement means drafted in the text, particularly in case OSPs do not comply with their obligations.

The study of these components will be accompanied by relevant legal literature, and with research from other disciplines, such as sociology, criminology, and computer sciences, that are concerned with CSAM. Therefore, the study relies on an instrumental approach to interdisciplinarity, so that the study of the legal framework is clarified by research results in other fields (Thompson Klein, 2017).

Results

Material scope

Defining illegal content

Provisions related to obligations of OSPs under the *Directive 2011/93/EU* relate to the offense of child pornography (Articles 21 and 25). Article 5 mandates Member States to criminalize the intentional (a) production; (b) acquisition or possession; (c) distribution, dissemination, or transmission; (d) offering, supplying, or making available of child pornography; and (e) knowingly obtaining access to child pornography by means of information and communication technology (ICT). Under *Directive 2011/93/EU*, the criminalization of child pornography is not fully harmonized, as Member States can adopt different rules regarding the private use of such material or depending on the age of sexual consent (see section defining "child"). Also, despite the existence of a European provision, transpositions by Member States still slightly differ, due to terminological variability as highlighted in the 2016 transposition report. In 2016, while most adopt the core terms, differences appear, such as Germany's use of "undertaking to retrieve" instead of "knowingly obtaining access" (Article 5(3) *Directive 2011/93/EU*), or Italy's use of "spreading" for "transmission" (Article 5(4) *Directive 2011/93/EU*). Similarly, France refers to "setting and recording" instead of "production" (Article 5(6) *Directive 2011/93/EU*) and the Czech Republic replaces "supplying" with "import," "selling," or "provision in another manner" (Article 5(5) *Directive 2011/93/EU*) (European Commission, 2016a). Despite the lack of more recent comparative analysis of national transpositions, the impact assessment of the *Recast of Directive 2011/*

Table 2. Summary of main comparative elements on obligations of OSP to fight against CSAM (presented in historical order).

Texts	Material scope	Personal scope	Obligations	Sanctions
Directive 2011/93/EU	Child pornography	Member States, targeting webpages	Removal/blocking of webpages	No provision
		Member States	Prevention and prohibition of advertisement	
AMSD	Child pornography as in Article 5(4) *Directive 2011/93/EU*	Member States, targeting video-sharing platform providers	Protect the general public from content whose dissemination constitutes a criminal offense	Effective and proportionate sanctions
DSA	Illegal content	Intermediary services providers	Order to act against illegal content Order to provide information	Up to 6% of total worldwide annual turnover in preceding financial year
		Hosting providers	Notice and action mechanism Notification of suspicions of criminal offenses	
		Online platforms	Prioritization of trusted flaggers Internal complaint-handling system	
		VLOP/SEs	Mitigation of risks	
Interim Regulation	Child pornography, pornographic performance and solicitation of children as in Article 2(c) and (e) and Article 6 *Directive 2011/93/EU*	Number-independent interpersonal communications services	Upon voluntary use of detection technologies: – Reporting content suspected or verified as CSA – Answer to LEAs' requests – Block, terminate, or suspend concerned service – Hash creation – Enhanced data protection obligations – Information, redress, and complaint obligations toward users	No provision

(*Continued*)

Table 2. (Continued).

Texts	Material scope	Personal scope	Obligations	Sanctions
CSAR Proposal	Child pornography, pornographic performance and solicitation of children as in Article 2(c) and (e) and Article 6 *Directive 2011/93/EU*	Hosting and interpersonal communications providers (including software applications store providers)	Assessment, mitigation, and reporting of risk of use for CSA Implementation of detection orders with technical, transparency, and user-related obligations Implementation of removal orders with technical, transparency and user-related obligations	Up to 6% of total worldwide annual turnover in preceding financial year
		Internet access service providers	Implementation of blocking orders with technical, transparency, and user-related obligations	
		All above mentioned providers	Establishment of a single point of contact Establishment of an EU legal representative if applicable Transparency obligations	
Recast of Directive 2011/93/EU	Child sexual abuse material	Member States, targeting webpages	Removal/blocking of webpages	No provision
		Member States	Prevention and prohibition of advertisement	

93/EU highlights such a persistent challenge for prosecution, particularly to ensure smooth cross-border cooperation and the criminalization of newer forms of CSAM offenses—for instance, "text and audio-based CSAM, live streaming, virtual reality and augmented reality CSAM, CSAM deepfakes, the use of digital currencies, and metaverse developments" (European Commission, 2024a, p. 27). Nevertheless, divergent transpositions issues could be circumvented if OSPs would refer to EU terminology.

The *Recast of Directive 2011/93/EU* mostly aims to update the vocabulary of the text and does not modify the content of the offense. Yet, the text clarifies that child pornography offenses, when committed by or on behalf and under the responsibility of an authorized organization acting in the public interest against child sexual abuse, shall not qualify as an offense (Articles 5.7 and 8). This exception allows for NGOs such as helplines to transfer content they receive to LEAs. Such an exception, although not explicitly provided for in the text, could apply as well to OSPs, if obliged by law to detect and transfer CSAM.

Differently, the *AMSD* aims only for OSPs in order to fight against the distribution, dissemination, and transmission of child pornography (Article 28b referring to Article 5.4 *Directive 2011/93/EU*). As a result, the *AMSD* has been criticized for not covering enough harmful content, due to its restrictive listing (Sorbán, 2023). Additionally, there is no plan to update vocabulary used in the *AMSD* to match with the *Recast of Directive 2011/93/EU*.

Both the *Interim Regulation* and the *CSAR Proposal* have extended the illegal content against which OSPs must act. The former text refers to online CSAM, which includes child pornography, pornographic performance, and solicitation of children (Articles 2(2) to (4) *Interim Regulation*). However, here, child pornography and pornographic performances do not refer to criminal offenses under *Directive 2011/93/EU* but to its definitions. Under the *Interim Regulation*, pornographic performances are ones of the typologies of CSAM. Differently, solicitation of children under the *Interim Regulation* refers to the offense under *Directive 2011/93/EU*. The *CSAR Proposal* refers, slightly differently, to CSAM, which includes child pornography and pornographic performances as described in the *Interim Regulation* but excludes the solicitation of children (Article 2(l) *CSAR Proposal*). Similarly, CSA performances are not classified as CSAM under Articles 2(3) and (4) *Recast of Directive 2011/93/EU*. Under the *CSAR Proposal*, CSAM can be known, meaning already registered in dedicated databases, or new (Article 2(m) and (n) *CSAR Proposal*). The online dissemination of CSAM and the solicitation of children constitute online CSA (Article 2(p) *CSAR Proposal*).

In addition to combatting CSAM, the *Interim Regulation* and the *CSAR Proposal* address the prevention and detection of the offense of online sexual solicitation of children, also known as grooming. Grooming is a "seductive process with the objective of befriending a child and subsequently preparing the child for sexual abuse" (Klimek, 2020, p. 8). According to Article 6.1 of *Directive 2011/93/EU*, it grooming is the intentional proposal by means of ICT "by an adult to meet a child who has not reached the age of sexual consent," of a meeting to commit CSA, including the production of CSAM. To qualify as an offense, the proposal must be followed by preparatory acts, such as buying a train ticket or booking an accommodation. The *Recast of Directive 2011/93/EU* clarifies that such a meeting can happen either online or in person (Article 6.1(a)). Grooming also encompasses the online solicitation of a child by an adult to attempt, "by means of information and communication technology, to commit the offences provided for in Article 5(2) [acquisition or possession] and (3) [knowingly obtaining access] by an adult soliciting a child who has not reached the age of sexual consent to provide" CSAM (Article 6.2).

Despite such a rather clear definition, the literature has shown the difficulty of identifying grooming due to its dynamics being unique and varied (de Santisteban et al., 2018; Kloess, Hamilton-Giachritsis, et al., 2019), especially since differences remain between grooming processes for in-person meeting and for the acquisition or access of CSAM (Soldino & Seigfried-Spellar, 2024). The second category of grooming might be easier to combat by OSPs, as the literature has shown that many scripts involve clear sexual intentions (Greene-Colozzi et al., 2020; Kleijn & Bogaerts, 2021). Yet, challenges might remain, as offenders might depict themselves as a child or peer of the child, which adds to the already mentioned age-related difficulties.

Conversely, the *DSA* broadly refers to illegal content in its provisions, as it remains a general framework. The text thus merely refers to activities not compliant with European Union or national law, which includes offenses under *Directive 2011/93/EU* (Article 3(h) *DSA*). However, Member States' transposition of these offenses may still show national specificities and differences, which complicates the uniform application of the DSA and cooperation among stakeholders (Bleakley et al., 2023; Holt et al., 2020). While a "specific definition of the illegality or harmfulness of content [. . .] is not possible" (Cole et al., 2021, pp. 125–127), some scholars have argued it could legitimize a form of private censorship of online content as OSPs would be able to justify the erasure of content based on broad criminal categories (Barata, 2021; Perarnaud, 2022). Although some scholars already discuss this issue (Drolsbach & Pröllochs, 2024; Fasel & Weerts, 2024), due to the novelty of the *DSA*, research is still required on its implementation and to analyze which definitions (e.g., international, European, national) are adopted by OSPs fighting against illegal content, particularly CSAM. These might be European, from Member States or from the European Union, or refer to international treaties (Council of Europe, 2007 *Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse*; United Nations, 2000 *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*). Given the terminological and criminal variability in the European Union, OSPs might differently prefer definitions from the country in which they are headquartered, often, the United States (*18 U.S. Code § 2252*).

This first analysis underlines that the different texts do not use harmonized categories nor refer, in a uniform way, to definitions or offenses as set out in *Directive 2011/93/EU*. Such a situation risks complicating the task of OSPs, which might have to refer to EU definitions and/or to national transpositions of offenses. In any case, two elements must be clarified: who classifies as a child and what materials are considered sexual abuse. The study of both elements underlines issues in harmonizing the way OSPs must understand CSAM.

Defining "sexual abuse material"

According to *Directive 2011/93/EU*, child pornography includes two types of sexual abuse material or visual depiction: (a) "a child engaged in real or simulated sexually explicit conduct" and (b) "the sexual organs of a child [depicted] for primarily sexual purposes" (Article 2(c)). Therefore, the text does not apparently encompass other materials such as text or audio messages that could be related to the sexual abuse of a child. Furthermore, *Directive 2011/93/EU* defines pornographic performances as "a live exhibition aimed at an audience, including by means of [ICT]," for the same two types of sexual abuse material (Article 2(e)). Performances are thus live material. However, the literature has criticized the term *child pornography* (Frangež et al., 2015; Interagency Working Group on Sexual Exploitation of Children, 2016). It creates

a comparison "with adult pornography, suggesting that Child Pornography is something other than the recording of child abuse" (Clough, 2012, p. 234).

As a result, the *Recast of Directive 2011/93/EU* offers to replace the term *child pornography* with "CSAM" and the term *pornographic performances* with "CSA performances." Furthermore, the category of CSAM is extended by adding "any material [. . .] intended to provide advice, guidance or instructions on how to commit" CSA or child solicitation (Article 2(c)(e)). The main advantage of the proposal seems to connect CSAM to the definition of CSA, which is not explicit under the current *Directive 2011/93/EU*. Indeed, the term *child pornography* does not refer to CSA, which is criminalized by Article 3. Changing the term *child pornography* to "CSAM" creates such a link. Under the currently applicable text, sexual abuse refers to intentionally "engaging in sexual activities with a child" or intentionally "coercing, forcing or threatening a child into sexual activities with a third party" (Articles 3.4 and 6). The *Recast of Directive 2011/93/EU* clarifies the notion of "sexual activities," by explicitly including "any act of vaginal, anal or oral penetration of a sexual nature, with any bodily part or object" (Article 3.7). However, enforcement practices will shed light on whether the sexual activities listed under a sexual abuse fully overlap with the notion of CSAM or if the latter is broader.

To classify CSA content, both the literature and practitioners rely on nonlegal typologies, such as the Combating Paedophile Information Networks in Europe (COPINE) typology (Quayle, 2008). Guidelines from the Sentencing Council in England and Wales rely on a simplified version that divides content into three categories (Martellozzo & DeMarco, 2020): (a) penetrative sexual activity, sexual activity with an animal or sadism, (b) nonpenetrative sexual activity, and (c) other indecent images (Sentencing Council, 2014). Therefore, engaging in sexually explicit conduct with a child, particularly when penetrative, seems to be straightforwardly classified as CSAM in relation to CSA offenses. However, the criminalization of nonpenetrative conduct is not harmonized under CSA offenses in the *Recast of Directive 2011/93/EU*. Although images such as youthful-adult pornography or images depicting naked children could classify as CSAM, they might not qualify as CSA. Furthermore, the practice shows the difficulty of classifying "indecent" images as well as proving their sexual purpose (Clough, 2012; Kloess, Woodhams, et al., 2019). Magistrates and practitioners specialized in this topic struggle to categorize potential CSAM. Therefore, such a decision would be even more complex for OSPs and their moderators. As national differences remain in the law and in practice on what qualifies as CSAM, OSPs "create their own definitions of abusive conduct to overcome obstacles arising from conflicting national laws" (Falduti & Griffo, 2024).

Defining "child"

Additionally, not all materials identified as CSAM nor all sexual activities involving a child will qualify as an offense. It is therefore of utmost importance to attend to the definition of "child" and to exceptions to criminalization.

Directive 2011/93/EU defines a child as "any person below the age of 18 years" (Article 2(a)), in accordance with international treaties (Sorbán, 2023). Yet, a CSAM-related offense does not only refer to such a threshold.

Firstly, Member States can criminalize sexual abuse material depicting a person "appearing to be a child" (Article 2(c)(iii)) or "realistic images of a child," such as drawings (Article 2(c)(iv)). The *Recast of Directive 2011/93/EU* adds to the concept of realistic images, reproductions, or representations of a child. Therefore, some States may create an exception to criminalizing when the person involved "was in fact 18 years of age or older at the time of

depiction" (Article 5.7) or when no child has been abused to create realistic images that are used for private use that do not risk being disseminated (Article 5.8). Currently, questions remain on the application of this exception to sexual deepfakes, involving only the faces of children and no underlying sexual abuse. AI-generated CSAM might also be trained based on real CSAM online. Therefore, aside from technical difficulties in identifying and removing it, virtual CSAM remains in a legal vacuum, mostly tackled by national law (S. Krishna et al., 2024; Maras & Logie, 2024; Olson, 2021; Ratner, 2021).

Secondly, certain sexual activities involving a child might not qualify as sexual abuse, depending on the age of sexual consent, "below which, in accordance with national law, it is prohibited to engage in sexual activities with a child" (Article 2(b)). Indeed, *Directive 2011/93/EU* mostly criminalizes sexual abuse depending on the age of sexual consent (Articles 3.4 and 6). The age, however, is irrelevant in the case of abuse of position of trust, authority, or influence of the perpetrator; abuse of a particularly vulnerable situation of the child; or when there is the use of coercion, force, or threats (Article 3.5). This distinction is slightly modified by the *Recast of Directive 2011/93/EU*. Sexual activities involving children are to be criminalized whenever the child is below the age of sexual consent or above it and did not consent to the act (Articles 3.4 and 8). This introduces consent as the determining element of a sexual offense. In the *Recast*, consent must be voluntarily given "as a result of the child's free will assessed in the context of the surrounding circumstances" (Article 3.9). Therefore, consent is highly contextual (Dowds, 2020; Setty, 2023).

Similarly, when it comes to CSAM, Member States may exclude the criminalization of "the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse" (Article 8.3). The *Recast of Directive 2011/93/EU* extends this exception to the access and dissemination of CSAM if the material exclusively involves consenting children above the age of sexual consent and potentially their peers (Articles 10.3 and 5). Consent is defined as under CSA (Article 10.5). The *CSAR Proposal* clarifies that giving consent to share a material once does not permit any additional sharing or distribution of the same image or video (Article 10.6).

Therefore, to verify that specific material could qualify as an offense, OSPs should assess the age of the person(s) depicted and the existence or lack of consent in parallel with the applicable law. However, OSPs might not have enough information to answer these questions and assess whether images are CSAM or not. The age of sexual consent concept "varies considerably between jurisdictions" (Clough, 2012, p. 213), ranging from 14 to 18 years old, as in 2017 in EU Member States (European Union Agency for Fundamental Rights, 2017). In comparison, most of the unique hashes identified globally by the IWF in 2023 regard children from age 7 to 13 years, for which consent and age are irrelevant to classify CSAM as an offense (IWF, 2024b). Yet, more than 140,000 hashes still concern children age 14 or older. For those under the jurisdiction of EU Member States, age and consent (or circumstances voiding consent) should be considered to assess whether the material is illegal or not. Also, both concepts of "age of consent" and "child" require identifying the age of the persons depicted, which faces many technical limits (Chaves et al., 2020; Lee et al., 2020; MacLeod et al., 2020). Age classifications still rely on limited data training sets, mostly identifying White children and leading to discriminatory results against children of color (Thakor, 2018). Even human identification, such as by medical experts, performs poorly and often requires additional

information (Kloess, Hamilton-Giachritsis, et al., 2019). The latter concept of consent may require additional information to assess its existence. In conjunction, these elements are particularly relevant to assess three situations—namely, erotic auto-depictions, self-produced juvenile pornography (depictions that are disseminated) and youthful-adult or "barely legal" pornography (Clough, 2012). Particularly, the *CSAR Proposal* does not consider potential consensual content, such as that self-generated between adolescents. The text has thus been criticized, due to the breadth of obligations of OSPs to "an extensive and invasive surveillance system" of children, such negatively affecting their fundamental rights (Neroni Rezende, 2024, p. 11). As some of the selected texts refer to the definition of CSAM and not to CSAM-related offenses, it conceals many complexities in the diversity of child sexuality (Kenny, 2018; Zhu, 2023) and allows OSPs to regulate behaviors instead of preventing offenses (Sonck & de Haan, 2014; van den Berg, 2014).

Personal scope

It should be noted here that neither *Directive 2011/93/EU* nor its *Recast* set a specific personal scope in their very broad provisions for Member States to create obligations on OSPs to fight against CSAM but merely refer to webpages. While many hosting services, including social media platforms, were already in existence —albeit less developed than today—when *Directive 2011/93/EU* was adopted, it is nonetheless surprising that its *Recast* retains the original wording instead of aligningwith contemporary EU digital law terminology (see Figure 1).

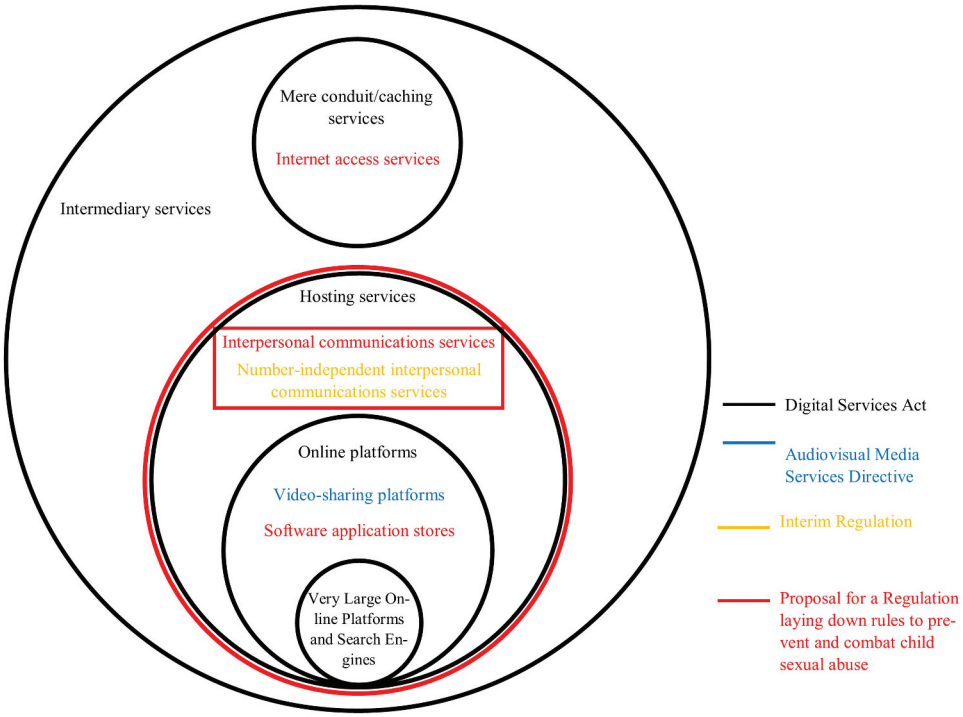

Figure 1. Summary of categories of OSPs obliged to fight against CSAM under the selected EU laws.

General categories of OSPs

The *DSA*, in its obligations to OSPs to fight against illegal content, according to a four-level regulation (Busch, 2022; Nüßing et al., 2022), refers to providers of intermediary services (Articles 9 and 10), of hosting services (Articles 16, 17, and 18), of online platforms (Articles 20, 21, and 22), and of very large online platforms or search engines (VLOP/SEs) (Articles 34 and 35). These providers must implement the *DSA* if they offer a service to recipients established or located in the European Union (Article 2.1). The *CSAR Proposal* relies on the same geographical connection to the EU (Article 2(g)) and definition of hosting services (Article 2(a)).

Under the *DSA*, the first category represents the broader one, including any providers of a service provided at a distance, by electronic means, through the transmission of data on individual request (Article 3(a) and (g) referring to Article 1.1(b) *Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services*). This includes many, if not all, online services. It includes services transmitting information in or providing access to a communication network (mere conduit), including if storing automatically and temporarily the information (caching), and services storing information (hosting) (Article 3(g)). Hosting services include social networks, online marketplaces, and so forth. Among hosting services, an online platform "stores and disseminates information to the public" at the request of the user (Article 3(i)), such as a social network; and a search engine "allows users to input queries in order to perform searches" of websites (Article 3(j)). Within those two categories, VLOP/SEs are designated by the European Commission when they "have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million" (Article 33.1). OSPs such as Amazon, Google (including YouTube), and Meta (including Facebook and Instagram), as well as adult-content websites—namely, Pornhub, XNXX, Stripchat, and XVideos—have been designated as VLOP/SEs (European Commission, 2024d).

Specific categories of OSPs

The *AMSD* introduces a specific type of online platform: video-sharing platform providers (VSPs) (Article 28b), such as YouTube. These host, on an electronic communication network, "content in video format, produced or uploaded by users and/or from a catalogue of a media service provider," organized by the provider while not bearing editorial responsibility for such content (Article 1(aa) and (da)).

The *Interim Regulation* refers to providers of NIICS, meaning enabling, via electronic communications networks, "direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons," "which does not connect [or enable communication] with publicly assigned numbering resources" (Article 2(1) referring to Articles 2(7), (4) and (5) *Directive (EU) 2018/1972 establishing the European Electronic Communications Code*). This category includes messaging (for instance, WhatsApp), videoconferencing (for instance, Zoom) and e-mail (for instance, Gmail) services that do not require a national phone number to register or use their services. More broadly, obligations to OSPs under the *CSAR Proposal* partially refer to providers of interpersonal communications services, whether they are number-based or number-independent, including if such service is ancillary to another service (Article 2(b)). This broader category includes messaging services connected to national phone numbers.

Interpersonal communications services allow for communication to a limited number of persons and not to the public; therefore, they do not qualify as online platforms.

The *CSAR Proposal* further refers to two other special categories of OSPs. Firstly, it refers to providers of software application stores, as an intermediated product or service (Article 2(d) referring to Article 2(14) *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector*). Secondly, it refers to providers of internet access service, offering "connectivity to virtually all end points of the internet" (ISPs) (Article 2(e) referring to Article 2(2) *Regulation (EU) 2015/2120 laying down measures concerning open internet access*). Under the *CSAR Proposal*, hosting services, interpersonal communications services, software applications stores, and ISPs are referred to as "relevant information society services," a category encompassing OSPs which must comply with specific obligations (Article 2(f)).

Adaptation of OSP categories to criminological realities

The multiplication of OSP categories complexifies the multiple layers of obligations to fight against CSAM. Criminological research reveals that offenders often leverage a range of OSPs and technologies that blend multiple functionalities, creating challenges for categorization and regulation. Despite specialized norms (*Interim Regulation*, *CSAR Proposal*) focusing on these specific categories, research shows that offenders still use traditional hosting services providers to access CSAM, such as peer-to-peer software and websites on the open web. Conversely, instant messaging services still can be used, albeit limitedly, for such purposes (Steel et al., 2022). Similar trends have been analyzed for the online distribution of CSAM (Cale et al., 2021). Yet, these specific categories might not fully account for the complexities and rapid evolution of technologies used in criminal activities (Shiau et al., 2024). For instance, research is raising awareness of the use of dating apps for CSAM-related offenses (Teunissen et al., 2022, 2024). These would generally qualify as a hosting service by storing information of their users. They might qualify as an online platform if profiles are shared with the public, although visibility can also be restricted depending on affordances. Part of these applications also offer interpersonal communications services, which are number-independent, although phone numbers can be used to register. Therefore, different services of a same provider might abide to different levels of obligations (see Sections Lex generalis and followings). Additionally, the criminological data underscore that offenders do not limit themselves to one single OSP category; rather, they benefit from the specific affordances of each platform. For example, encrypted chat functionalities, file-sharing capabilities, and forums that can distribute links to encrypted files are all used interchangeably or in combination, complicating efforts to apply a rigid classification framework and prevention and prosecution efforts in silos (Steel et al., 2022). In practice, LEAs will thus have to seek collaboration with many types of providers and services that might abide different obligations. Furthermore, it remains open to discussion how darknet platforms and services should be classified within these categories, despite research demonstrating their increasing role in facilitating CSAM offenses (Internet Watch Foundation, 2024a; Leclerc et al., 2021; Steel et al., 2022). Finally, these categories might face limitations as new services will appear or due to the displacement of offenders and potential victims (Quayle, 2020; Steel et al., 2022).

Obligations

Lex generalis

Under the *DSA*, providers of intermediary services, the largest category of OSPs, can "in good faith and in a diligent manner, carry out *voluntary* own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content," without triggering their liability (Article 7).

Conversely, providers of intermediary services must act against illegal content and provide information regarding specific recipient(s) of their service, upon order of a national judicial or administrative authority (Articles 9 and 10). The national authority must specify the territorial scope of an order to act against illegal content (e.g., national or European) (Article 9.2(b)). However, these provisions do not create a legal basis for national authorities to order OSPs to tackle CSAM. Therefore, despite the *DSA* being directly applicable, LEAs will require a specific legal basis to produce orders to act against CSAM, which might be found under the EU CSAM-specific framework or at the national level. OSPs might remain free to choose whether, for example, they erase the content, render the content invisible to users, or block the account. As a result of implementing either or both types of orders, the OSPs must inform the affected user along with a statement of reason and the possibilities of redress (Article 9.5). Yet, national civil and criminal procedural law can supersede these provisions when regulating these orders (Articles 9.6 and 10.6).

Providers of hosting services receive further obligations. They must implement mechanisms "to allow any individual or entity to notify them of the presence on their service of" potential illegal content (Article 16). Such a notice results in the knowledge of these OSPs of the content, therefore, the OSP must act upon the information or would be liable (Article 16.3 in relation with Article 6). These OSPs must confirm the reception of the notice (Article 16.4) as well as notify the person to whom the notice relates, such as the account holder, with the possibilities of redress (Articles 16.5 and 6). Furthermore, the OSP must provide a statement of reasons to "any affected recipients of the service" in case of restrictions of the provision of the service (Article 17.1). This means that not only the account holder should be informed but, potentially, the persons affected by the illegal content, such as the child or their guardians, in case of CSAM. However, that is only if the OSP knows "the relevant electronic contact details" of the persons (Article 17.2)—for instance, if the account of the affected person is tagged under the publication or if their automated systems recognize the face of the featured person. Under this notice mechanism, providers of online platforms must give priority to those submitted by trusted flaggers, designated nationally, for their "particular expertise and competence" (Article 22). Some countries have already designated entities fighting against CSA, such as ECPAT Sweden (European Commission, 2024e). However, it remains incoherent that only providers of online platforms must prioritize trusted flaggers' notice and not all providers of hosting services.

When providers of hosting services acquire knowledge, for example through a notice, of information "giving rise to a suspicion that a criminal offense involving a threat to the life or safety of a person," which is the case for CSAM, the service has the obligation to promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned—meaning where the offense is suspected to have taken place or where the suspected offender or victim resides or is located (Article 18).

In addition to the notice mechanism, providers of online platforms (Article 19) must implement "an effective internal complaint-handling system that enables them to lodge complaints, electronically and free of charge" (Article 20). The reporting individual (e.g., victim or guardian) or entity (e.g., NGO or State entity for minors' protection) could thus debate the decision of these providers to not consider a specific content as CSAM. Alternatively, the affected user could also dispute that an erased content was CSAM. After the provider has decided on the complaint, they must inform the affected person of any out-of-court dispute settlement body available for further remedy (Article 21). Also, online platforms must "put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service" (Article 28).

Additionally, VLOP/SEs must mitigate risks to fundamental rights (Article 35), particularly in the case of systemic risks of "the dissemination of illegal content through their services" or negative effects in relation to the protection of minors (Article 34.1(a) and (d)). Yet, the *DSA* does not mandate specific mitigation measures and merely gives examples, such as adapting moderation processes and introducing tools to protect minors, including age verification and parental control tools (Article 35.1(c) and (j)). Despite the broadness of this provision, it remains relevant as adult-content websites have been designated as VLOPs (European Commission, 2024d), which can host both legal and illegal content— whether depicting minors or adults. So far, the European Commission has issued multiple requests for information toward pornography companies designated as VLOPs concerning illegal content, the protection of minors, transparency reports, and advertisement repositories (European Commission, 2024b, 2024c). However, the Commission appears to face challenges in engaging with these actors, as some dispute their designation as VLOPs (Krempl, 2025) and given they have provided only limited information—prompting the Commission to launch a formal investigation in May 2025 (European Commission, 2025b).

Finally, due diligence provisions mainly address transparency through reporting obligations. Yet, they might remain pertinent as VLOP/SEs will have to report mitigating measures (Article 37.3), including those aimed at mitigating hosting and dissemination of CSAM if identified as a systemic risk (Article 42.4). Some provisions could also participate indirectly in the fight against CSAM by supporting digital literacy, including of minors—for example, in ensuring that terms and conditions of use are user-friendly (Article 14.1 and 3).

Lex specialis: The AMSD

The amended *AMSD* mandates Member States to adopt national legislation to ensure that VSPs "take appropriate measures to protect," on the one hand, minors from content "which may impair their physical, mental or moral development" (Article 28b.1(a)). Among harmful content, those most harmful include "gratuitous violence and pornography" and must be subject to the strictest measures (Article 6a.1 and Article 28b.3). As CSAM will not anymore be considered pornography, it can still fall under the first category. On the other hand, VSPs must receive national obligations to protect the general public from content classified as a criminal offense under Union law, including the distribution, dissemination, or transmission of child pornography (Article 28b.1(c)). Measures must be content- and harm-specific as well as depend on the audience to be protected; at the same time, they must be "practicable and proportionate" depending on the capacities of the VSP (Article 28b.3). These measures may include the explicit prohibition of illegal content in terms and conditions of use or implementing a reporting mechanism with an explanation of the

reasons for the decision taken as well as a complaint mechanism (Article 28b.3(a), (d), (e), and (i)). These measures largely overlap with now-mandatory obligations under the *DSA*. VSPs could also implement age verification systems or parental control systems to protect minors (Article 28b.3(f) and (h)), which neither are mandatory under the *DSA*. Concerned OSPs have fluidly implemented a wide diversity of obligations from transposing national laws, mainly through age verification systems and moderation of uploaded content, particularly on adult websites, some of which are now VLOP/SEs (European Regulators Group for Audiovisual Media Services, 2022).

Lex specialis: CSAM-specific frameworks

Since *Directive 2011/93/EU*, Member States must adopt national measures to promptly remove or block access to "web pages containing or disseminating child pornography" (Article 25). The text does not clarify whether national authorities would directly implement these powers or order OSPs to remove or block content (European Commission, 2016b, 2024a). Furthermore, Member States must prevent or prohibit content advertising the opportunity or organization of travel arrangements to commit a child pornography offense or CSA (Article 21). The *Recast of Directive 2011/93/EU* does not modify these provisions except for updating the terminology (Articles 26 and 30). Therefore, this framework provides no obligation on OSPs to fight CSAM.

More important are the *Interim Regulation* and the *CSAR Proposal*. The *Interim Regulation* creates an exception to the principle of confidentiality of communications (Article 5 *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector*) to allow the use of "specific technologies for the processing of personal and other data to the extent strictly necessary to detect online [CSA] on their services and report it and to remove online [CSAM] from their services" (Article 1.1 *Interim Regulation*). For these purposes, NIICS providers can process both content (e.g., the text of the message) and traffic data (e.g., data to identify the sender and receiver of the message) (Article 3.1(a)(iii)). Research has shown that traffic data can already provide relevant information to detect CSAM, although with some limitations (Guerra & Westlake, 2021; B. Westlake & Guerra, 2023). The *Interim Regulation* specifies that such technologies cannot be used to scan audio communications to detect CSAM (Article 1.2). The *Interim Regulation* seems to focus on textual communications, potentially including images, while the scanning of video communications lies in a legal gap. NIICS providers could potentially scan video communications, as long as they are not processing the audio. This also enables offenders to circumvent the efforts of OSPs, as it could incentivize them to use audio messages instead of text messages, particularly in grooming strategies. Yet, the *Interim Regulation* creates a mere possibility for concerned OSPs to implement such technologies.

If they implement these technologies, NIICS providers must report suspected CSA to LEAs or relevant organizations, respond to related requests, block or suspend the user while ensuring redress, and create a hash of the content (Article 3.1(h) and (j)). Reporting of new CSAM requires mandatory prior human confirmation (Article 3.1(g)(iii)).

Further obligations relate to technical standards, also vaguely defined. The technologies must follow state-of-the-art standards and be as privacy-friendly as possible, focusing on detecting CSA patterns without revealing full message content (Article 3.1(b)). Particularly, technologies to detect potential grooming should be limited to detect "relevant key

indicators and objectively identified risk factors such as age difference and the likely involvement of a child" (Article 3.1(f)). They must also limit the rate of errors, and in case of errors, providers must rectify consequences of those (Article 3.1(e)).

To ensure compliance with technical standards, NIICS providers receive enhanced data protection obligations. To ensure the proportionality of the interference to the right to privacy, these technologies must realize enhanced assessment under the *GDPR*, including a data protection impact assessment and consultation with the national data protection authority (Article 3.1(c) and (d) referring to Articles 35 and 36 *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, *GDPR*).

Finally, NCIIS providers receive additional obligations relevant to ensuring transparency of their action and necessary rights to their users. Providers must comply with further obligations, such as to ensure human oversight and intervention (Article 3.1(g)(ii)). Providers further need to inform users of the implementation of these technologies, similar to information obligations under the *GDPR* (Article 3.1(g)(v) *Interim Regulation*, in parallel with Articles 12, 13, and 22 *GDPR*), and inform users of outcomes of moderation processes, including implementing redress mechanisms, similar to the complaint mechanism provided in the *DSA* (Article 3.1(g)(iv) and (vi) *Interim Regulation*). Also, NIICS providers must report to the European Commission on the use of these technologies to comply with the transparency principle (Article 3.1(g)(vii)).

Crafting new obligations to OSPs, the *CSAR Proposal* firstly ensures that hosting and interpersonal communications services providers assess, mitigate, and report the risk for their services to be used for CSA (Articles 3 to 5). For example, mitigation measures include, in close wording to the *DSA*, adapting moderation or recommender systems as well as terms and conditions, or ensuring cooperation with LEAs or trusted flaggers, although the personal scope of the *CSAR Proposal* (hosting and interpersonal communications services providers) diverges from the one of the *DSA* on trusted flaggers (online platforms) (Article 4.1). Software application providers receive additional mitigation measures, such as the mandatory introduction of age verification or assessment measures (Article 6.1).

Secondly, hosting and interpersonal communications services providers must implement detection orders, issued by national judicial or administrative authorities where there is "evidence of a significant risk of the service being used for the purpose of online [CSA]" (Article 7.4(a)). To qualify as such a risk, in relation to known CSAM, the authority must justify that the service is likely used or has been used in the past 12 months "to an appreciable extent" for CSAM dissemination (Article 7.5). Relating to grooming, the authority shall use the same justifications, as long as it relates to an interpersonal communications service provider (Article 7.7). Relating to new CSAM, the authority must additionally prove the existence of an order to detect known CSAM or of "a significant number of reports" for known CSAM (Article 7.6). The execution of these orders is conducted through detection technologies (Article 10.1), which must comply with similar standards as in the *Interim Regulation* (Article 10.4 and 5).

Thirdly, hosting and interpersonal communications services providers must implement removal orders issued by national judicial or administrative authorities for content qualified as CSAM (Article 14.1). Providers must comply within 24 hours of the receipt of removal orders (Article 14.2). Given this very short period of time, OSPs might automate these

procedures. The provider must inform the user, including a statement of reasons, and provide possibilities of redress, obligations that overlap with those in the *DSA* (Article 15).

Fourthly, whenever hosting and interpersonal communications services providers receive information of potential CSAM, they must report it to the EU Centre created for such purposes (Article 12.1 and Article 13). The provider must inform the user of such a report and possibilities of redress, as in the *DSA* (Article 12.2). The provider must offer a notice mechanism, an obligation that overlaps with the *DSA* (Article 12.3). The question remains if an additional mechanism or an explicit reporting function should be designed specifically for CSAM. Also, whenever these OSPs implement one of the preceding obligations, they must preserve the data related to it as long as necessary and up to 12 months (Article 22).

Differently, ISPs must implement blocking orders issued by national judicial or administrative authorities by preventing "users from accessing known [CSAM] indicated by all uniform resource locators" (URL) on a database processed by the EU Centre (Article 15.1). These orders, which can last up to 5 years (Article 15.6), can be issued whenever the service has been used during the past 12 months, to an appreciable extent, to access CSAM (Article 15.4). As under the removal order, providers must inform users, particularly of means of redress, and implement complaints mechanisms (Articles 18.3 and 4).

On a procedural note, providers of relevant information society services, meaning all these obliged under the *CSAR Proposal*, must establish a single point of contact for direct communication, as well as a legal representative in the European Union if they do not have their main establishment there (Articles 23 and 24). Similar OSPs will already receive the same obligations under national transpositions of *Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings*. Given that the instruments are different (a regulation and a directive), there is an increased risk of lack of harmonization among Member States and the designation of different points of contact depending on the applicable instrument. For instance, OSPs might establish their *CSAR Proposal* point of contact in Country A to receive removal orders while receiving European Production Orders within a CSAM investigation in their point of contact in Country B based on national transpositions.

It should be mentioned here that the *CSAR Proposal* has faced substantial criticism from national (Morte Ferrer, 2022) and EU perspectives (EDPB & EDPS, 2022; EDPS, 2024; Legal Service of the Council of the EU, 2023; Quintel, 2023) and legal and technical scholars (Bleakley et al., 2023; Collective, 2024; Neroni Rezende, 2024), many of which could be applied to the *Interim Regulation*. Concerns center on its proportionality with respect to human rights, especially the right to privacy. Critics highlight the regulation's vague terminology, such as the undefined "significant risk" (Article 7) and the ambiguous threshold for issuing detection orders. Similarly, the regulation's lack of clarity regarding acceptable error rates and definitions of "reliable detection technologies" exacerbates concerns about transparency and accuracy (Neroni Rezende, 2024), which could lead to inconsistent enforcement and subjective interpretation. Additionally, artificial intelligence (AI) systems implemented for these purposes lack transparency (Deldari et al., 2024), and the role of the *AI Act* in mitigating opacity remains to be seen (*Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence*) (Busuioc et al., 2023; Tzimas, 2023; Varošanec, 2022). More broadly, these

obligations on OSPs might result in generalized surveillance through permanent scanning of a majority of online content while discouraging high encryption standards (Neroni Rezende, 2024; Pingen, 2022).

Doubts also persist about its technical feasibility and the risk of errors. False positives are known risks, as demonstrated by cases like Operation Ore, in which individuals linked to flagged CSAM were wrongly prosecuted due to fraudulent credit card use for illicit materials (Anderson, 2022). Even hashing techniques have shown flaws in detecting known CSAM due to the potential for slight alterations of images to evade detection and ineffectiveness at detecting new CSAM (Lee et al., 2020; B. Westlake et al., 2022). The effectiveness of filtering techniques, necessary for a blocking order, has also been largely debated (Martellozzo & DeMarco, 2020), especially in view of the large quantities of inaccurate data in EU operational databases (European Union Agency for Fundamental Rights Ed., 2018). Furthermore, these technologies will still face the technical limits of encrypted and anonymous data (Teunissen & Napier, 2022). From another practical perspective, the literature has largely questioned the capabilities of OSPs and LEAs to process the amount of data flagged by technologies implemented under detection orders (Anderson, 2022; Neroni Rezende, 2024; Quintel, 2022). Recent discussions on client-side scanning highlight this tension: Although CSS could help detect known and unknown CSAM even in encrypted services and aid prevention by warning potential victims, it also risks creating broad security vulnerabilities, privacy intrusions, and scope creep for other forms of content monitoring, while facing significant technical and legal challenges in reliably distinguishing illegal material at scale Abelson et al. (2024); Bhardwaj et al. (2024); Geierhaas et al. (2023); Twenning and Baier (2024).

Enforcement

The selected texts show a trend in the instruments chosen by the EU legislators, from directives to an increased number of regulations, "as correctional mechanisms to complement non-existent or not uniform Member States laws" (Sorbán, 2023, p. 185), particularly when it comes to OSPs' obligations to fight against CSAM. Enforcement mechanisms under directives are generally broad and left to the discretion of Member States. The *AMSD* only mentions sanctions and enforcement mechanisms as part of codes of conduct (Article 4a.1(d)), which is surprising considering the principle of legality of penalties: Those must be passed as legal provisions. Therefore, this provision might not refer to sanctions by Member States on noncompliant OSPs but to sanctions by OSPs on noncompliant users such as offenders. The text entirely refers to national law for enforcement of obligations of VSPs (Article 28b.5). *Directive 2011/93/EU* does not provide for sanctions against OSPs, as it remains very vague on their obligations.

Conversely, regulations tend to guide Member States in setting sanctions, which will be implemented at national level. The *Interim Regulation* does not provide for sanctions, as OSPs remain free to implement technologies to fight against CSAM.

The *DSA* requires Member States to be able to fine OSPs for a compliance failure up to "6% of the annual worldwide turnover [. . .] in the preceding financial year" (Article 52.3). When the national enforcement mechanism offers a delay for the OSP to comply, Member States should be able to impose a penalty payment of up to "5% of the average daily worldwide turnover or income [. . .] in the preceding financial year per day" (Article

52.4). Regarding VLOP/SEs, the European Commission is entitled to investigate any noncompliance and to directly fine them in the same amounts (Articles 74.1 and 76). It remains to be seen whether these penalties will be implemented against OSPs that are noncompliant in fighting against CSAM as a type of illegal content.

The *CSAR Proposal* mandates national authorities to receive enforcement powers to ensure the compliance of OSPs with the regulation (Articles 27 to 29). In case of noncompliance, penalties must be passed at the national level, with fines up to "6% of the annual income or global turnover of the preceding business year," or period payments of up to "5% of the average daily global turnover [...] in the preceding financial year per day" (Article 35).

Aside from civil sanctions for noncompliance with their obligations to fight against CSAM, such a noncompliance might result in criminal sanctions against OSPs. Since *Directive 2011/93/EU*, Member States must consider sanctioning legal persons for committing or participating in CSAM-related offenses (Article 12 and 13). The *Recast of Directive 2011/93/EU* mandates Member States to criminalize a new conduct, the intentional operation or administration of an online service "conceived to facilitate or encourage the commission" of CSA or CSAM-related offenses (Article 8). The *Recast of Directive 2011/93/EU* also increases criminal sanctions on legal persons, with fines of not less than 1% to 5% of the total worldwide turnover (Article 14.2 and 3). However, OSPs benefit from an exemption of liability, as long as they have no knowledge of hosting illegal content such as CSAM (Article 6 *DSA*). Therefore, it remains to be seen the level of proof required for the new offense under the *Recast of Directive 2011/93/EU* and the interplay between the liability regime of the *DSA* and the obligations under the *Interim Regulation* and the *CSAR Proposal*. If OSPs comply with obligations under the *CSAR Proposal*, they are not liable for CSAM-related offenses (Article 19 *CSAR Proposal*). Conversely, noncompliance might result in criminal liability.

Conclusion

A systematic analysis shows that EU law imposes an increasingly complex set of obligations on OSPs to fight against CSAM, which interact through both general (lex generalis) and specific (lex specialis) frameworks, often creating overlaps, gaps, and legal uncertainty.

Firstly, the material scope of these obligations has expanded from narrowly defined criminal offenses to broader categories of illegal or harmful content. This shift risks blurring the line between what is criminally punishable and what is merely undesirable online. For example, not all content captured by the term CSAM in EU law will necessarily qualify as CSAM-related offenses, especially where national age of consent laws and consent by adolescents come into play. This can lead to the over-removal of content, including consensual self-generated sexual content exchanged between peers (so-called sexting), which—although socially sensitive—may not always amount to an offense. OSPs, operating across multiple jurisdictions, face the difficult task of determining the legality of such content based on context they often do not have, potentially restricting children's freedom of expression rather than protecting them from abuse. OSPs might wish to adopt EU harmonized definitions of CSAM, although these do not entirely overlap with criminal provisions on CSAM. Legal challenges in determining what is CSAM are to be added to technological challenges, as this content is often context dependent or due to the lack of

reliable results—for example, for age identification. This leads to heightening the risk of false positives, whether because content is not legally criminalized in the concerned country or due to technological limitations. False positives might increasingly burden LEAs due to mandatory reporting obligations, which is already challenging in the United States (Office of Justice Programs & Office of Juvenile Justice and Delinquency Prevention, 2024). Additionally, further work will be necessary to study the potential overlap of CSAM and CSAM-related offenses with the new EU offense of nonconsensual sharing of intimate or manipulated material (Dodge & Spencer, 2018; Gangi et al., 2022) (Article 5 *Directive (EU) 2024/1385 on combating violence against women and domestic violence*).

Secondly, the personal scope of obligations is highly fragmented. Whereas the *DSA* focuses on hosting services, online platforms and VLOP/SEs, CSAM-specific frameworks such as the *CSAR Proposal* add obligations for interpersonal communications services and other categories, such as software application stores. Yet, offenders often use multiple providers simultaneously and providers often offer multiple services, which might complicate enforcement, as undermines siloed regulatory approaches must be leveraged to combat complex illegal phenomena.

Thirdly, while the *DSA*, *Interim Regulation*, *CSAR Proposal*, and *AMSD* all create obligations that partially overlap—such as notice-and-action mechanisms, reporting obligations, and risk mitigation—they differ in terminology, definitions of illegal content, subjects of the obligations, and technical measures required. This fragmentation may increase compliance burdens for OSPs by requiring them to implement multiple overlapping frameworks, such as the *DSA* and the *CSAR Proposal*, whose obligations are often similar but differ in material scope (covering all illegal content versus CSAM specifically). Importantly, the *AMSD* cannot be overlooked: although its obligations may appear limited, Member States have already transposed its provisions into national laws, which will need to be revised to align with newer frameworks like the *CSAR Proposal*—potentially leading to legal conflicts between national and EU law. Additionally, technical obligations under the selected texts, particularly the *DSA*, the *Interim Regulation* and the *CSAR Proposal*, remain vague, which calls into question what technical safeguards are available against general surveillance and private power to regulate online behaviors and accepted content and which should be reported to LEAs (Decoster, 2024). This is especially relevant given that penalties, when they exist, are particularly high, which might incentivize OSPs to over-moderate content, with a risk to freedom of expression and information.

Therefore, EU law progressively extends obligations on OSPs beyond criminal law, into preventive and risk-based frameworks. Yet, the EU legislators, especially in pending negotiations, must ensure that EU law remains transversally coherent, especially in its definitions. While a streamlined system might be unimaginable due to the general framework set by the *DSA*, duplications and overlaps will have to be clarified. To this end and to ensure that children are safe online, regulatory bodies, especially the European Commission (European Commission, 2025a), the forthcoming EU Centre to Prevent and Counter Child Sexual Abuse, and data protection authorities will have to support the implementation of all these legal frameworks, particularly by OSPs and national law enforcement authorities. In the meantime, due diligence obligations could incentivize OSPs to adopt more-transparent moderation policies grounded in human rights standards and criminal definitions to ensure robust human review alongside automated tools and to engage with child protection experts to design context-sensitive approaches.

Despite these technological solutions and collaborations, so far mostly reactive to the commission of the crimes, prevention and a child-centered approach should be strengthened. Generally, OSPs' current and future obligations stem from a prohibitive mindset, aimed at prohibiting or removing content, which might fail to implement a victim-centric policy, supporting, for example, children's needs and fundamental rights (Phippen & Bond, 2024). By relying on more-diverse scientific results, all stakeholders, and particularly EU institutions, could move beyond myths on the reality of children's life online and a technological solutionism in fighting against CSAM (Gerrard, 2025; Morozov, 2013; ten Hulsen, 2025), especially by ensuring collaboration among all stakeholders, including LEAs, child protection institutions, schools and other education and leisure institutions, and parents (Anderson, 2022).

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Salomé Lannier http://orcid.org/0009-0003-3650-7866

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., Diffie, W., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Teague, V., & Troncoso, C. (2024). Bugs in our pockets: The risks of client-side scanning. *Journal of Cybersecurity*, *10*(1), tyad020. https://doi.org/10.1093/cybsec/tyad020

Anderson, R. (2022). *Chat control or child protection?* (No. 2210.08958). arXiv. https://doi.org/10.48550/arXiv.2210.08958

Anillo, I., Feldman, D., & Kennedy, T. (2023). A global outlook on child sexual abuse and sexually explicit material online during COVID-19: Trends and interdisciplinary prevention methods. *Journal of Child Sexual Abuse*, *32*(8), 921–939. https://doi.org/10.1080/10538712.2023.2285960

Barata, J. (2021). Obligations, liabilities and safeguards in content moderation. *Verfassungsblog: On Matters Constitutional*. https://doi.org/10.17176/20210302-154101-0

Bélair, G., Fortin, F., Chopin, J., & Chartrand, É. (2024). The dynamics of internet sexual solicitation: Examining the criminal careers of online groomers. *Deviant Behavior*, 1–14. https://doi.org/10.1080/01639625.2024.2408472

Bhardwaj, D., Guthoff, C., Dabrowski, A., Fahl, S., & Krombholz, K. (2024). Mental models, expectations and implications of client-side scanning: An interview study with experts. *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1–24). https://doi.org/10.1145/3613904.3642310

Bleakley, P., Martellozzo, E., Spence, R., & DeMarco, J. (2023). Moderating online child sexual abuse material (CSAM): Does self-regulation work, or is greater state regulation needed? *European Journal of Criminology*, *21*(2), 231–250. https://doi.org/10.1177/14773708231181361

Broadhurst, R. (2019). Child sex abuse images and exploitation materials. In E. R. Leukfeldt & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 310–336). Routledge. https://doi.org/10.4324/9780429460593-14

Busch, C. (2022). Regulating the expanding content moderation universe: A European perspective on infrastructure moderation special issue: Governing the digital space. *UCLA Journal of Law and Technology*, *27*(2), 32–79.

Busuioc, M., Curtin, D., & Almada, M. (2023). Reclaiming transparency: Contesting the logics of secrecy within the AI act. *European Law Open*, *2*(1), 79–105. https://doi.org/10.1017/elo.2022.47

Cale, J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). *Crime commission processes in child sexual abuse material production and distribution: A systematic review* (No. 617; trends and issues in crime and criminal justice, pp. 1-22). Australian Institute of Criminology. https://search.informit.org/doi/abs/10.3316/informit.721282335565713

Chaves, D., Fidalgo, E., Alegre, E., Alaiz-Rodríguez, R., Jáñez-Martino, F., & Azzopardi, G. (2020). Assessment and estimation of face detection performance based on deep learning for forensic applications. *Sensors*, *20*(16), Article 16. 4491. https://doi.org/10.3390/s20164491

Chopin, J., & Décary-Hétu, D. (2023). Dark web pedophile site users' cybersecurity concerns: A lifespan and survival analysis. *Journal of Criminal Justice*, *86*, 102060. https://doi.org/10.1016/j.jcrimjus.2023.102060

Clough, J. (2012). Lawful acts, unlawful images: The problematic definition of child pornography. *Monash University Law Review*, *38*(3), 213–245.

Cole, M. D., Etteldorf, C., & Ullrich, C. (2021). *Updating the rules for online content dissemination-legislative options of the European Union and the digital services act proposal*. Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748925934

Collective. (2024. May 2). *Joint statement of scientists and researchers on EU's new proposal for the child sexual abuse regulation*. https://nce.mpi-sp.org/index.php/s/eqjiKaAw9yYQF87

Decoster, N. (2024). The policing and reporting of online child sexual abuse material: A scoping review. *International Review of Penal Law*, *95*(2), 323–366.

Deldari, E., Thakkar, P., & Yao, Y. (2024). Users' perceptions of online child abuse detection mechanisms. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1–26. https://doi.org/10.1145/3637424

de Santisteban, P., Del Hoyo, J., Alcázar-Córcoles, M. Á., & Gámez-Guadix, M. (2018). Progression, maintenance, and feedback of online child sexual grooming: A qualitative analysis of online predators. *Child Abuse and Neglect*, *80*, 203–215. https://doi.org/10.1016/j.chiabu.2018.03.026

Dodge, A., & Spencer, D. C. (2018). Online sexual violence, child pornography or something else entirely? Police responses to non-consensual intimate image sharing among youth. *Social & Legal Studies*, *27*(5), 636–657. https://doi.org/10.1177/0964663917724866

Dowds, E. (2020). Towards a contextual definition of rape: Consent, coercion and constructive force. *Modern Law Review*, *83*(1), 35–63. https://doi.org/10.1111/1468-2230.12461

Drolsbach, C. P., & Pröllochs, N. (2024). Content moderation on social media in the EU: Insights from the DSA transparency database. *Companion Proceedings of the ACM Web Conference 2024* (pp. 939–942). https://doi.org/10.1145/3589335.3651482

Dushi, D. (2018). Combating the live-streaming of child sexual abuse and sexual exploitation: A need for new legislation. In J. Hunsinger, L. Klastrup, & M. M. Allen (Eds.), *Second international handbook of internet research* (pp. 1–23). Springer Netherlands. https://doi.org/10.1007/978-94-024-1202-4_43-1

EDPB & EDPS. (2022. July 28). *Joint opinion 04/2022 on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*. EU. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

EDPS. (2024. January 24). *Opinion 8/2024 on the proposal for a regulation amending regulation (EU) 2021/1232 on a temporary derogation from certain ePrivacy provisions for combating CSAM*. EU.

Edwards, G., Christensen, L., Rayment McHugh, S., & Jones, C. (2021). *Cyber strategies used to combat child sexual abuse material* (No. 636; trends & issues in crime and criminal justice). Australian Institute of Criminology. https://doi.org/10.52922/ti78313

European Commission. (2016a). *Extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography* (report No. COM(2016) 871 final). EU.

European Commission. (2016b). *Implementation of the measures referred to in article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children*

and child pornography (report No. COM(2016) 872 final). EU. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016DC0872

European Commission. (2020). *Eu strategy for a more effective fight against child sexual abuse* (communication No. COM(2020) 607 final). EU.

European Commission. (2022). *A digital decade for children and youth: The new European strategy for a better internet for kids (BIK+)* [communication]. EU. COM/2022/212 final.

European Commission. (2024a). *Impact assessment report accompanying the document Proposal for a directive 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 (recast)* (Commission staff working document No. SWD(2024) 33 final). EU.

European Commission. (2024b. June 13). *Commission sends request for information on illegal content and protection of minors to Pornhub, XVideos and Stripchat under the Digital Services Act*. https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-illegal-content-and-protection-minors-pornhub-xvideos-and

European Commission. (2024c. October 18). *Commission requests information under the Digital Services Act to Pornhub, Stripchat and XVideos on their transparency reports and advertisement repositories*. https://digital-strategy.ec.europa.eu/en/news/commission-requests-information-under-digital-services-act-pornhub-stripchat-and-xvideos-their

European Commission. (2024d. October 18). *Supervision of the designated very large online platforms and search engines under DSA*. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

European Commission. (2024e. October 21). *Trusted flaggers under the Digital Services Act (DSA)*. https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa

European Commission. (2025a. May 13). *Commission publishes draft guidelines on protection of minors online under the Digital Services Act*. https://digital-strategy.ec.europa.eu/en/news/commission-publishes-draft-guidelines-protection-minors-online-under-digital-services-act

European Commission. (2025b. May 27). *Commission opens investigations to safeguard minors from pornographic content under the DSA*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1339

European Regulators Group for Audiovisual Media Services. (2022). *The implementation(s) of article 28b AVMSD: National transposition approaches and measures by video-sharing platforms* (consistent implementation and enforcement of the audiovisual media services Directive framework No. Deliverable 1). EU.

European Union Agency for Fundamental Rights. (2017. November 14). *Consent for sexual activity with an adult* [European Union Agency for Fundamental Rights]. https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/consent-sexual-activity-adult

European Union Agency for Fundamental Rights (Ed.). (2018). *Under watchful eyes: Biometrics, EU IT systems and fundamental rights*. Publications Office. https://doi.org/10.2811/136698

Falduti, M., & Griffo, C. (2024). Ontological models for representing image-based sexual abuses. *Computer Law & Security Review*, *54*, 105999. https://doi.org/10.1016/j.clsr.2024.105999

Fasel, M., & Weerts, S. (2024). Can Facebook's community standards keep up with legal certainty? Content moderation governance under the pressure of the digital services act. *Policy & Internet*, *16*(3), 588–606. https://doi.org/10.1002/poi3.391

Finkelhor, D., Turner, H., Colburn, D., & Mitchell, K. J. (2024). Persisting concerns about image exposure among survivors of image-based sexual exploitation and abuse in childhood. *Psychological Trauma: Theory, Research, Practice, & Policy*, *17*(Suppl 1), S88–S93. https://doi.org/10.1037/tra0001815

Frangež, D., Klancnik, A. T., Karer, M., Ludvigsen, B.-E., Kończyk, J., Perez, F. R., Veijalainen, M., & Lewin, M. (2015). The importance of terminology related to child sexual exploitation. *Revija Za Kriminalistiko In Kriminologijo*, *66*(4), 291–299.

Gangi, O., Giacometti, M., & Gilen, A. (2022). Diffusion non consentie de contenus à caractère sexuel et diffusion d'images d'abus sexuels de mineurs: Entre distinctions et chevauchements, quelles implications d'un point de vue légal, criminologique et psycho-social? *Revue de la Faculté de Droit de l'Université de Liège*, *2022*(3), 635–674.

Geierhaas, L., Otto, F., Häring, M., & Smith, M. (2023). Attitudes towards client-side scanning for CSAM, terrorism, drug trafficking, drug use and tax evasion in Germany. *2023 IEEE Symposium on Security and Privacy (SP)*, 217–233. https://doi.org/10.1109/SP46215.2023.10179417

Georgieva, I., Koops, B.-J., Schermer, B., & van der Hof, S. (Eds.). (2019). *Sweetie 2.0: Using artificial intelligence to fight webcam child sex tourism* (1st ed.). T.M.C. Asser Press: Imprint: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-288-0

Gerrard, Y. (2025). *The kids are online confronting the myths and realities of young digital life* (1st ed.). University of California Press.

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse and Neglect*, *80*, 238–248. https://doi.org/10.1016/j.chiabu.2018.03.031

Graef, I., & van der Sloot, B. (Eds.). (2024). *The legal consistency of technology regulation in Europe* (1st ed.). Hart Publishing.

Greene-Colozzi, E. A., Winters, G. M., Blasko, B., & Jeglic, E. L. (2020). Experiences and perceptions of online sexual solicitation and grooming of minors: A retrospective report. *Journal of Child Sexual Abuse*, *29*(7), 836–854. https://doi.org/10.1080/10538712.2020.1801938

Guerra, E., & Westlake, B. G. (2021). Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites. *Child Abuse and Neglect*, *122*, 105336. https://doi.org/10.1016/j.chiabu.2021.105336

Gurriell, M. (2021). Born into porn but rescued by Thorn: The demand for tech companies to scan and search for child sexual abuse images. *Family Court Review*, *59*(4), 840–854. https://doi.org/10.1111/fcre.12613

Henry, C. (2020). Designing effective digital advertisements to prevent online consumption of child sexual exploitation material. *Journal of Child Sexual Abuse*, *29*(8), 877–899. https://doi.org/10.1080/10538712.2020.1841354

Holt, T. J., Cale, J., Leclerc, B., & Drew, J. (2020). Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. *Aggression & Violent Behavior*, *55*, 101464. https://doi.org/10.1016/j.avb.2020.101464

Husovec, M. (2024). *Principles of the Digital Services Act* (1st ed.). Oxford University Press.

Interagency Working Group on Sexual Exploitation of Children. (2016). *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*. ECPAT International.

Internet Watch Foundation. (2024a). *Geographical hosting: URLs | IWF, 2023 Annual Report*. https://www.iwf.org.uk/annual-report-2023/trends-and-data/geographical-hosting-urls/

Internet Watch Foundation. (2024b). *Unique image analysis | IWF, 2023 annual report*. https://www.iwf.org.uk/annual-report-2023/trends-and-data/unique-image-analysis/

Kenny, D. T. (2018). *Children, sexuality, and child sexual abuse*. Routledge. https://doi.org/10.4324/9781315109329

Klamert, M., & Loewenthal, P.-J. (2019). Article 288 TFEU. In M. Kellerbauer, M. Klamert, & J. Tomkin (Eds.), *The EU treaties and the Charter of fundamental rights: A commentary*. Oxford University Press. https://doi.org/10.1093/oso/9780198759393.003.432

Kleijn, M., & Bogaerts, S. (2021). Sexual offending pathways and chat conversations in an online environment. *Sexual Abuse*, *33*(8), 871–890. https://doi.org/10.1177/1079063220981061

Klimek, L. (2020). European responses criminalising online solicitation of children for sexual purposes. *Balkan Social Science Review*, *16*, 7–21. https://doi.org/10.46763/BSSR201607k

Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2019). Offense processes of online sexual grooming and abuse of children via Internet communication platforms. *Sexual Abuse*, *31*(1), 73–96. https://doi.org/10.1177/1079063217720927

Kloess, J. A., Woodhams, J., Whittle, H., Grant, T., & Hamilton-Giachritsis, C. E. (2019). The challenges of identifying and classifying child sexual abuse material. *Sexual Abuse*, *31*(2), 173–196. https://doi.org/10.1177/1079063217724768

Krempl, S. (2025. February 20). *Digital services act: User figures for porn platforms in the EU collapse*. Heise Online. https://www.heise.de/en/news/Digital-Services-Act-User-figures-for-porn-platforms-in-the-EU-collapse-10290281.html

Krishna, A. (2021). Internet.gov: Tech companies as government agents and the future of the fight against child sexual abuse. *California Law Review*, *109*, 1581. https://doi.org/10.15779/Z38KW57J9B

Krishna, S., Dubrosa, F., & Milanaik, R. (2024). Rising threats of AI-driven child sexual abuse material. *Pediatrics*, *153*(2), e2023063954. https://doi.org/10.1542/peds.2023-063954

Leclerc, B., Drew, J., Holt, T., Cale, J., & Singh, S. (2021). *Child sexual abuse material on the darknet: A script analysis of how offenders operate* (No. 627; trends & issues in crime and criminal justice). Australian Institute of Criminology. https://doi.org/10.52922/ti78160

Lee, H.-E., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*, *34*, 301022. https://doi.org/10.1016/j.fsidi.2020.301022

Legal Service of the Council of the EU. (2023). *Opinion on the proposal for a regulation laying down rules to prevent and combat child sexual abuse (No. 8787/23)*. EU.

MacLeod, L., King, D., & Dempster, E. (2020). A review of age estimation research to evaluate its inclusion in automated child pornography detection. In K. Arai, S. Kapoor, & R. Bhatia (Eds. Intelligent Computing: Proceedings of the 2020 Computing Conference (Vol. 1. pp. 566–580). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-52249-0_38

Maras, M.-H., & Logie, K. (2024). Countering the complex, multifaceted nature of nude and sexually explicit deepfakes: An Augean task? *Crime Science*, *13*(1), 31. https://doi.org/10.1186/s40163-024-00226-6

Martellozzo, E., & DeMarco, J. (2020). Exploring the removal of online child sexual abuse material in the UK: Processes and practice. *Crime Prevention and Community Safety*, *22*(4), 331–350. https://doi.org/10.1057/s41300-020-00099-2

Maxwell, F., Salter, M., & Peleg, N. (2024). 'To say report it, well, it seems a little useless': Evaluating Australians' expectations of online service providers and reducing online child sexual exploitation. *Policy & Internet*, *16*(2), 384–410. https://doi.org/10.1002/poi3.378

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism* (1st ed.). PublicAffairs.

Morte Ferrer, R. (2022). La propuesta de reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores. Poca luz y muchas sombras. *La Ley Privacidad*, *14*(octubre–diciembre), 16.

Neroni Rezende, I. (2024). The proposed regulation to fight online child sexual abuse: An appraisal of privacy, data protection and criminal justice issues. *International Review of Law, Computers and Technology*, 1–22. https://doi.org/10.1080/13600869.2024.2324548

Nüßing, C., Oehm, T., Arncken, D., & Grünwald, A. (2022. October 4). *The EU digital services act-Europe's new regime for content moderation*. Lexology. https://www.lexology.com/library/detail.aspx?g=297caa4e-686c-452c-a527-c56fb3fba7ee

Office of Justice Programs & Office of Juvenile Justice and Delinquency Prevention. (2024). *Report to the committees on appropriations national center for missing and exploited children (NCMEC) transparency*. US Department of Justice.

Olson, A. (2021). The double-side of deepfakes: Obstacles and assets in the fight against child pornography notes. *Georgia Law Review*, *56*(2), [i]–892.

Papakonstantinou, V., & De Hert, P. (2024). *The regulation of digital technologies in the EU: Act-ification, GDPR mimesis, and EU law brutality at play*. Routledge.

Paul, C., Manjunatha, S., Lakshmi Pa, A., & Sharma, G. (2024). A study on the information transfer and long-term psychological impact of child sexual abuse. *Georgian Medical News*, *348*, 28–31.

Perarnaud, C. (2022. July 1). Pour automatiser la censure, cliquez ici. *Le Monde diplomatique*. https://www.monde-diplomatique.fr/2022/07/PERARNAUD/64826

Phippen, A., & Bond, E. (2024). Why do legislators keep failing victims in online harms? *International Review of Law, Computers and Technology*, 1–20. https://doi.org/10.1080/13600869.2023.2295100

Pingen, A. (2022). Controversial proposal on combating child sexual abuse online. *Eucrim - The European Criminal Law Associations' Forum, 2/2022*, 91/92.

Prichard, J., Wortley, R., Watters, P. A., Spiranovic, C., Hunn, C., & Krone, T. (2022). Effects of automated messages on internet users attempting to access "barely legal" pornography. *Sexual Abuse*, *34*(1), 106–124. https://doi.org/10.1177/10790632211013809

Quayle, E. (2008). The COPINE project. *Irish Probation Journal*, *5*, 65–83.

Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum*, *21*(3), 429–447. https://doi.org/10.1007/s12027-020-00625-7

Quayle, E., & Koukopoulos, N. (2019). Deterrence of online child sexual abuse and exploitation. *Policing: A Journal of Policy and Practice*, *13*(3), 345–362. https://doi.org/10.1093/police/pay028

Quintel, T. (2022). European Union · the Commission proposal on combatting child sexual abuse-confidentiality of communications at risk? *European Data Protection Law Review*, *8*(2), 262–272. https://doi.org/10.21552/edpl/2022/2/13

Quintel, T. (2023). European Union · renewed concerns about compliance of the proposed 'regulation to prevent and combat child sexual abuse' with essence of right to data protection: The Council legal service opinion. *European Data Protection Law Review*, *9*(2), 173–183. https://doi.org/10.21552/edpl/2023/2/12

Ratner, C. (2021). When "sweetie" is not so sweet: Artificial intelligence and its implications for child pornography. *Family Court Review*, *59*(2), 386–401. https://doi.org/10.1111/fcre.12576

Salter, M., Wong, T., Breckenridge, J., Scott, S., Cooper, S., & Peleg, N. (2021). *Production and distribution of child sexual abuse material by parental figures* (trends & issues in crime and criminal justice no. 616). Australian Institute of Criminology. https://doi.org/10.52922/ti04916

Sentencing Council. (2014. April 1). *Possession of indecent photograph of child/indecent photographs of children - sentencing* [Sentencing Council]. https://www.sentencingcouncil.org.uk/offences/magistrates-court/item/possession-of-indecent-photograph-of-child/

Setty, E. (2023). Young people and sexual consent: Contextualising 'miscommunication' amid 'grey areas' of ambiguity and ambivalence. *Sex Education*, *25*(1), 155. https://doi.org/10.1080/14681811.2023.2259321

Shiau, A. Y. A., Holden, O. L., Musacchio, S., Talwar, V., & Wit-Williams, S. D. (2024). Online child sexual exploitation and the role of computer-mediated communication: A scoping review. *Journal of Child Sexual Abuse*, 1–24. https://doi.org/10.1080/10538712.2024.2388655

Soldino, V., & Seigfried-Spellar, K. C. (2024). Criminological differences between contact-driven and online-focused suspects in online child sexual grooming police reports. *Child Abuse and Neglect*, *149*, 106696. https://doi.org/10.1016/j.chiabu.2024.106696

Sonck, N., & de Haan, J. (2014). Safety by literacy? Rethinking the role of digital skills in improving online safety. In S. van der Hof, B. van den Berg, & B. Schermer (Eds.), *Minding minors wandering the web: Regulating online child safety* (pp. 89–104). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-005-3_5

Sorbán, K. (2023). An elephant in the room-EU policy gaps in the regulation of moderating illegal sexual content on video-sharing platforms. *International Journal of Law and Information Technology*, *31*(3), 171–185. https://doi.org/10.1093/ijlit/eaad024

Steel, C., Newman, E., O'Rourke, S., & Quayle, E. (2022). Technical behaviours of child sexual exploitation material offenders. *Journal of Digital Forensics, Security & Law*, *17*(1). https://doi.org/10.15394/jdfsl.2022.1794

Stringhi, E. (2024). The due diligence obligations of the digital services act: A new take on tackling cyber-violence in the EU? *International Review of Law, Computers and Technology*, 1–15. https://doi.org/10.1080/13600869.2023.2295101

ten Hulsen, L. (2025). Digital fixes and techno-solutionism: The EU's tech-based battle against child sexual abuse. *New Journal of European Criminal Law*, *16*(2), 154–175. https://doi.org/10.1177/20322844251348131

Teunissen, C., Boxall, H., & Napier, S. (2022). *The sexual exploitation of Australian children on dating apps and websites* (no. 658; trends and issues in crime and criminal justice, pp. 1-19). Australian Institute of Criminology. https://doi.org/10.52922/ti78757

Teunissen, C., & Napier, S. (2022). *Child sexual abuse material and end-to-end encryption on social media platforms: An overview* (No. 653; Trends & Issues in Crime and Criminal Justice, pp. 1-19).

Australian Institute of Criminology. http://proxy.bnl.lu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=sih&AN=158128576&site=ehost-live&scope=site

Teunissen, C., & Napier, S. (2023). *The overlap between child sexual abuse live streaming, contact abuse and other forms of child exploitation* (No. 671; Trends & Issues in Crime and Criminal Justice). Australian Institute of Criminology.

Teunissen, C., Thomsen, D., Napier, S., & Boxall, H. (2024). *Risk factors for receiving requests to facilitate child sexual exploitation and abuse on dating apps and websites* (trends & issues in crime and criminal justice no. 686). Australian Institute of Criminology. https://doi.org/10.52922/ti77291

Thakor, M. (2018). Digital apprehensions: Policing, child pornography, and the algorithmic management of innocence. *Catalyst: Feminism, Theory, Technoscience*, *4*(1), Article 1. 1–16. https://doi.org/10.28968/cftt.v4i1.29639

Thakor, M., Sabnam, S., Ueno, R., & Zaslow, E. (2023). To search and protect? Content moderation and platform governance of explicit image material. *MIT Case Studies in Social and Ethical Responsibilities of Computing*, (Summer 2023). https://doi.org/10.21428/2c646de5.cdecbadf

Thompson Klein, J. (2017). Typologies of interdisciplinarity: The boundary work of definition. In R. Frodeman (Ed.), *The Oxford Handbook of interdisciplinarity* (2nd ed. pp. 21–34). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198733522.013.3

Tolbaru, C.-E. (2022). Fight against sexual abuse and online exploitation of children - key priority at the European Union level section: Law. *International Journal of Legal and Social Order*, *1*(1), 347–356. https://doi.org/10.55516/ijlso.v1i1.94

Twenning, L., & Baier, H. (2024). Towards arbitrating in a dispute-on responsible usage of client-side perceptual hashing against illegal content distribution. Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (pp. 105–114). https://doi.org/10.1145/3655693.3655712

Tzimas, T. (2023). Algorithmic transparency and explainability under EU law. *European Public Law*, *29*(4), 385–411. https://doi.org/10.54648/EURO2023021

Ugwudike, P., Roth, S., Lavorgna, A., Middleton, S. E., Djohari, N., Tartari, M., & Mandal, A. (2024). Sharenting and social media properties: Exploring vicarious data harms and sociotechnical mitigations. *Big Data & Society*, *11*(1), 20539517231219243. https://doi.org/10.1177/20539517231219243

van den Berg, B. (2014). Colouring inside the lines: Using technology to regulate children's behaviour online. In S. van der Hof, B. van den Berg, & B. Schermer (Eds.), *Minding minors wandering the web: Regulating online child safety* (pp. 67–85). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-005-3_4

Varošanec, I. (2022). On the path to the future: Mapping the notion of transparency in the EU regulatory framework for AI. *International Review of Law, Computers and Technology*, *36*(2), 95–117. https://doi.org/10.1080/13600869.2022.2060471

WeProtect Global Alliance. (2024). *Global threat assessment 2023 assessing the scale and scope of child sexual exploitation and abuse online, to transform the response.*

Westlake, B., Brewer, R., Swearingen, T., Ross, A., Patterson, S., Michalski, D., Hole, M., Logos, K., Frank, R., Bright, D., & Afana, E. (2022). *Developing automated methods to detect and match face and voice biometrics in child sexual abuse videos* (no. 648; Trends & Issues in Crime and Criminal Justice). Australian Institute of Criminology. https://doi.org/10.52922/ti78566

Westlake, B. G. (2020). The past, present, and future of online child sexual exploitation: Summarizing the evolution of production, distribution, and detection. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 1225–1253). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_52

Westlake, B., & Guerra, E. (2023). Using file and folder naming and structuring to improve automated detection of child sexual abuse images on the dark web. *Forensic Science International: Digital Investigation*, *47*, 301620. https://doi.org/10.1016/j.fsidi.2023.301620

Zhu, G. (2023). European legislators' attitudes toward childhood sexuality from the perspective of age of consent legislation. *European Journal of Criminology*, *20*(4), 1309–1330. https://doi.org/10.1177/14773708211046195