laws

MDPI

Article

The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe

Katalin Parti [1,*] and Judit Szabó [2]

[1] Department of Sociology, Virginia Tech, Blacksburg, VA 24061, USA
[2] Division of Criminal Law Sciences, National Institute of Criminology, 1122 Budapest, Hungary; judit.szabo@okri.hu
* Correspondence: kparti@vt.edu

Abstract: Although the escalation in online child sexual abuse material (CSAM) is not a novel problem, recent digital proliferation has brought about new alarming challenges in addressing the issue. CSAM poses significant risks to children and society in general, the most serious being the long-lasting harmful effects on depicted victims. The already distressing problem is exacerbated by the worldwide appearance and spread of AI-driven or virtual CSAM, as AI offers a fast and increasingly profitable means for the sexual exploitation of children. The paper aims to provide a comprehensive review of current legislative measures focusing the European Union for combating online CSAM. With a particular focus on AI-driven CSAM, we will systematically evaluate the effectiveness and applicability of these regulations in addressing virtual CSAM. The paper will conclude with policy recommendations to address identified gaps in the European legislative framework concerning virtual CSAM.

Keywords: online; child sexual abuse material (CSAM); artificial intelligence; AI-driven CSAM; regulation; Europe; European Union

Citation: Parti, Katalin, and Judit Szabó. 2024. The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws* 13: 67. https://doi.org/10.3390/laws13060067

Academic Editors: Terry Carney and Patricia Easteal

Received: 15 August 2024
Revised: 10 October 2024
Accepted: 24 October 2024
Published: 30 October 2024

1. Introduction

Child Sexual Abuse Material (CSAM) refers to any visual or textual content that depicts or involves the sexual abuse or exploitation of children. CSAM can include photos, videos, audio, drawings, and even digital manipulations of children in sexual contexts (ECPAT 2016). In the context of this paper, "traditional" CSAM depicts real, existing children in sexually exploitative situations. These materials involve actual victims, and their creation typically involves the direct abuse or exploitation of children. "Virtual" CSAM, on the other hand, either features actual children's digitally manipulated images or entirely fictional situations with fictional characters. This paper utilizes Krishna et al.'s (2024, p. 1) definition of virtual CSAM or AI-driven CSAM, according to which virtual CSAM has two main forms: AI-generated CSAM and AI-manipulated CSAM. The term AI-generated CSAM indicates new sexual images of fictional children, while AI-manipulated CSAM refers to images and videos of real children altered into sexually explicit content.

Although the phenomenon can be referred to by various terms, CSAM is the preferred term in legal and policy contexts globally (ECPAT 2016), as it clearly conveys the abusive nature of the material and reflects the resulting trauma to the child. Some legal frameworks use different terms, such as child pornography (including in the United States under 18 U.S.C. § 2256), which is defined as "any visual depiction of sexually explicit conduct involving a minor" (Lindenhovius 2022). The U.K. is another example where Indecent and Prohibited Images of Children (The Crown Prosecution Service 2018) is a definition used in legal proceedings, which makes it illegal to create, distribute, or possess indecent images of children. This terminology often extends beyond images to videos and other forms

of digital content (Kloess et al. 2017). Australia, yet another country, uses the term child exploitation material, focusing on the exploitation aspect under the Criminal Code Act 1995 (Krone et al. 2017). Diverse terms aside, many experts and child protection organisations are encouraging the term "child sexual abuse material" because the term "child pornography" downplays the abuse and implies consent or active involvement by the child, which is inherently not possible (ECPAT 2016).

CSAM is widespread all over the world. In 2023, CyberTipline, the hotline of the National Center for Missing and Exploited Children (NCMEC 2023), received 35.9 M reports of suspected online child sexual abuse cases involving the possession, creation, or distribution of CSAM. This trend represents an 18.4% increase in reporting from 2021. In 2023, CyberTipline received over 186,000 reports regarding online enticement—a more than 300% increase from 2021 (NCMEC 2023). Online enticement or grooming is a form of exploitation involving an individual who communicates online with someone they believe to be a child with the intent to commit a sexual offence or abduction. In 2023, 91.7% of reports to CyberTipline involved the upload of CSAM by users outside of the U.S., 4.5% of reports involved U.S. users, and 3.8% had an unknown origin, indicating that most of these severe crimes occurred cross-border and their investigation requires a concerted effort from law enforcement and internet service providers (NCMEC 2023). The majority of reports received were related to the circulation of CSAM, but the data also indicated a continued rising trend in reports of the use of generative artificial intelligence (GAI) in child sexual exploitation. Offenders use GAI for AI-driven CSAM in distinct ways: (i) they can create deepfake sexually explicit images or videos based on any photograph of a real child (AI-manipulated CSAM), or (ii) generate CSAM depicting computer-generated depictions of children engaged in graphic sexual acts (AI-generated CSAM). In 2023, CyberTipline received 4700 reports of CSAM or other sexually exploitative content related to GAI (NCMEC 2023).

With the radical shift to online spaces during lockdowns prompted by the recent coronavirus pandemic, there was a significant upsurge in CSAM. Compared to the 16.9 M reports received by CyberTipline in 2019, the number of reports increased to 21.7 M in 2020 and reached a staggering 29.3 M in 2021 (NCMEC 2021). Other sources (e.g., WeProtect Global Alliance 2023; Interpol 2022) corroborate the trend. CSAM surged during the pandemic due to a combination of increased internet usage, social isolation, and the closure of schools, which left children more vulnerable and exposed to online predators, as well as the limited ability of law enforcement to monitor and respond to these crimes amidst the broader public health crisis (European Commission 2022; Interpol 2022). Lovett went as far as using the term "silent epidemic" (Lovett 2024) to refer to the growing trend of child sexual abuse cases under the pandemic.

Europe is one of the regions which have given significant consideration to the issue of child exploitation, particularly child sexual exploitation, and have adopted a robust and multifaceted approach that involves comprehensive legislation, dedicated institutions, and cross-border co-operation. The European Union (EU) has implemented stringent legal frameworks such as Directive 2011/93/EU[1], which mandates member states to adopt measures against the sexual abuse and exploitation of children and child pornography. The Directive ensures a harmonized approach across the EU, enhancing legal consistency and enforcement capabilities. Furthermore, specialized agencies like Europol's European Cybercrime Centre (EC3) and initiatives such as the EU Internet Forum (European Commission 2024) work collaboratively to prevent and combat online child sexual abuse by facilitating information sharing and operational co-operation among member states. Additionally, the EU has invested in public awareness campaigns and support systems for victims, including hotlines and helplines in the form of the joint Insafe-INHOPE network of Safer Internet

[1] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA. (OJ L 335 of 17 December 2011). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0093 (accessed on 25 October 2024).

Centres in the European Union[2]. These combined efforts reflect the EU's comprehensive commitment to protecting children from exploitation and ensuring their safety and well-being. Furthermore, the EU is politically, legislatively, and geographically central in the fight against cybercrime due to its comprehensive legal frameworks such as the General Data Protection Regulation (GDPR)[3] and the Directive on Security of Network and Information Systems (NIS 2 Directive)[4], established institutions like Europol and the European Union Agency for Cybersecurity (ENISA), and its strategic location bridging eastern and western cybercrime networks, and facilitating extensive international co-operation and enforcement efforts across borders (Murphy 2024; Bendiek and Maat 2019; Markopoulou et al. 2019).

One of the most significant challenges in the fight against online child sexual exploitation is balancing online safety with citizens' privacy and freedoms, particularly in the age of GAI. The severity of harm caused by virtual CSAM remains a subject of debate, complicating regulatory and enforcement efforts. As GAI technology advances, its capacity to create highly realistic images indistinguishable from real photos increases, which raises concerns about potential psychological impacts and ethical implications (Linz and Imrich 2001; Ali et al. 2024). These advancements necessitate robust legal frameworks to address the creation and distribution of AI-driven CSAM while ensuring that privacy rights are not excessively compromised (Thiel et al. 2023, p. 8; Internet Watch Foundation 2023). In addition, stricter surveillance and data monitoring measures necessary for detecting and preventing crimes often conflict with fundamental privacy rights, raising concerns over the potential misuse of AI technologies for mass surveillance and the erosion of individual freedoms (Fuster and Jasmontaite 2020; Pavlova 2020; Korff 2019).

CSAM poses significant risks to children and society in general. Children depicted on CSAM are victims of sexual abuse even if no physical force is involved, even if they know the abuser, and even if the material is self-made. With the recording of the sexual abuse, victims experience further and ongoing victimisation, potentially resulting in even more serious mental health consequences that may impact their adulthood as well. These include constant feelings of guilt and shame (Gewirtz-Meydan et al. 2018; Svedin and Back 2003), humiliation (Gewirtz-Meydan et al. 2019), worry about being recognized in public (Gewirtz-Meydan et al. 2018; NCMEC 2022), fear that others would think that they had been willing participants, and mental difficulties like anxiety, depression, paranoia, sleeping problems, hypervigilance, suicidal ideation or attempts, other self-harm, low body image, and relationship and sexual difficulties (Canadian Centre for Child Protection 2017). Many victims also feel pressure to co-operate and non-disclose (Silbert 1989). Feelings of guilt, shame, and humiliation are intensified by the fact of being photographed or recorded (Hunt and Braid 1990). Being out on the internet, recordings cause an ongoing experience of revictimisation, a feeling that the abuse never ends (Gewirtz-Meydan et al. 2018).

Pornographic material, including CSAM, is used to groom and harass children and youth, and their exposure to such material also has several harmful effects, such as social maladjustment, psychological problems, violence, normalization of sexual pathology, and changes to sexual behavior (Taylor 2018). The normalization of sexting and other risky sexual behaviors is also a possible consequence of the spread of CSAM (Foothills Child Advocacy Centre n.d.). According to Taylor (2018), the rise of child-on-child sexual assault may be causally linked to children's access to pornography.

Besides the effects on victims and children exposed to CSAM, other possible adverse consequences are also mentioned in academic discourse. Such a potentially harmful, albeit

[2] https://www.betterinternetforkids.eu/ (accessed on 16 July 2024).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. Available online: https://gdpr-info.eu/ (accessed on 25 October 2024).

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (accessed on 25 October 2024).

somewhat debated, effect is CSAM being a gateway or a fuel to hands-on sexual offending. Although some scholars argue that virtual CSAM may help to prevent contact child abuse by providing an acceptable alternative outlet for paraphilic sexual urges (Diamond et al. 2011; van Es 2016), a more widely supported view is that consuming CSAM might actually increase the risk of contact offending (e.g., Insoll et al. 2022; Johnson 2020). Although the controversy is far from being resolved, it seems plausible to assume that CSAM consumption can act as a risk factor for contact abuse in the case of those who are already predisposed to offend (Seto et al. 2001), but not so much for those without a previous history of contact child sexual abuse (Hörnle et al. 2024; Endrass and Rossegger 2010).

Another growing body of research deals with the phenomena of desensitisation and normalisation that may occur as a result of continued exposure to CSAM, which may lead to a preference for more extreme and abusive child exploitation material (Seigfried-Spellar and Rogers 2013) and can undermine internal inhibitions against abusing children (Russell and Purcell 2008). Empirical evidence suggests that pornography consumers can escalate into using CSAM because of boredom due to habituation, even in the absence of pedophilic preferences (Knack et al. 2020; Seigfried-Spellar and Rogers 2013).

The already distressing problem of CSAM is exacerbated by the worldwide appearance and spread of AI-driven CSAM. Besides the revictimisation of former victims and the victimisation of others (e.g., famous children, by practically flooding the internet), virtual CSAM puts tremendous strain on police and law enforcement systems, also impeding the identification and protection of real child victims of sexual exploitation (Krishna et al. 2024; NCMEC 2024).

The paper aims to provide a comprehensive review of current European legislative measures in combating online CSAM. With a particular focus on AI-driven CSAM, we will systematically evaluate the effectiveness and applicability of these regulations in addressing virtual CSAM images. The paper will conclude with policy recommendations to address identified gaps in the EU's legislative framework concerning virtual CSAM.

2. Method and Sample

Applying two distinct but complementary research methods, the paper aims to provide a comprehensive understanding of the effectiveness of legal regulations designed to address these harms. The integrative literature review (research method 1) forms the foundation of the study by synthesising existing knowledge on the topic, specifically the legal and regulatory landscape concerning traditional and virtual CSAM in Europe. As Shuck (2011) describes, this method is useful in evolving fields with diverse perspectives, such as online child exploitation, where both technological advancements and legal responses are rapidly changing. The review's purpose is to create a comprehensive understanding of how these harms are currently regulated and to highlight areas where new insights or knowledge gaps exist. The literature review employs the triangulation method, which involves cross-verifying findings through multiple sources to enhance the validity and reliability of the review. In this context, the review analyses various data sources (e.g., academic journal articles, legal reports, directives). By doing so, the literature review captures a broader and more nuanced understanding of the issues around CSAM and AI-generated content. The review was conducted by identifying sources from databases like EBSCO and ProQuest, using specific keywords to capture relevant publications between 2014 and 2024, using keywords "online child sexual abuse/CSAM/online child sexual exploitation/CSE + legi*/lega* + Europe," "online child sexual abuse/CSAM/online child sexual exploitation/CSE + legi*/lega* + challenge," and online child sexual abuse/CSAM/online child sexual exploitation/CSE + artificial intelligence/AI" published between 2014 and 2024, which made it possible to select 71 sources including peer reviewed journal articles and reports.

Several key factors explain why we chose to review the literature over the 10-year timeframe from 2014 to 2024. During this time, the EU has implemented crucial regulatory frameworks, and introduced new strategies like the EU Strategy for a More Effective

Fight Against Child Sexual Abuse (European Commission 2020). The period also reflects technological advancements, particularly the rise of artificial intelligence and deepfake technologies and their implications for detecting and combating CSAM (Okolie 2023). As AI technologies began playing a more prominent role in law enforcement, this decade marks a critical time for the intersection of technology and regulation. Additionally, the Lisbon Treaty (2009) fundamentally reshaped the EU's legal landscape, giving more legislative power to the Union in areas of justice and home affairs (Carrera and Guild 2014). By focusing on the post-2014 period, the review captures the EU's evolving legal capacity to harmonise laws related to child protection and CSAM. By extending the literature review to 2024, the research captures current developments and ongoing discussions about CSAM regulation, including the COM (2022) 209 Final[5], the role of platforms under the Digital Services Act (DSA 2022)[6], and how evolving legislation addresses emerging AI-driven threats. This future-oriented approach ensures the literature review remains relevant for ongoing policy discussions.

Following the literature review, the paper undertakes a legal analysis (research method 2) to assess the effectiveness and applicability of current legal regulations addressing both traditional and virtual CSAM. The legal analysis directly engages with the content and structure of the relevant laws and regulations identified in the literature review, aiming to address the research questions. The analysis focused on key international and EU regulations, directives, proposed legislation, and non-binding treaties that govern CSAM and AI-driven content. The selection criteria for the instruments were guided by relevance to the research questions. Once identified, each legal instrument was assessed based on its applicability to traditional CSAM and AI-driven content, especially in addressing deepfake technologies, and considering both strengths and potential weaknesses of existing legal frameworks. The analysis sought to evaluate the effectiveness of these laws in practice, such as the enforcement mechanisms in place, gaps in addressing AI-driven content, and challenges encountered by law enforcement agencies. Both methods are designed to answer the research questions comprehensively. The literature review offers a broad overview of the regulatory landscape and its challenges, while the legal analysis provides a detailed evaluation of specific laws, ensuring the study offers actionable insights and policy recommendations.

The instruments we analyzed in the manuscript span international, European, and technological regulatory frameworks. Thus, we used the European Convention on the Rights of the Child as an international convention, the Budapest and Lanzarote Conventions as Council of Europe regulatory frameworks, European Union proposed legislations (COM (2022) 209 Final), directives (European Directive 2011/93/EU), and regulations (DSA 2022) to provide a broad spectrum for addressing traditional CSAM as well as the novel challenges posed by AI-driven content.[7]

---

[5] Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN&qid=1652451192472 (accessed on 25 October 2024).

[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance). PE/30/2022/REV/1. OJ L 277, 27 October 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065 (accessed on 25 October 2024).

[7] The recently enacted Artificial Intelligence Act of the EU (*Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828*) does not directly aim to enhance AI-driven identification of victims and offenders in CSAM investigations. While it sets stringent regulations on AI use, particularly prohibiting most real-time biometric surveillance in public spaces, the AIA focuses more on regulating AI risks rather than providing tools to aid law enforcement in tackling CSAM. The AIA's primary goal is to control how AI can be used, with exceptions granted only in specific, tightly regulated scenarios. Such an exception is the one regulated in Section 5(1) d of the AIA, which states that the otherwise prohibited use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement can be used for the targeted search for specific potential victims of crime, including missing children, for the prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons or of a terrorist attack and for the detection, localisation, identification, or prosecution of a perpetrator or suspect of a criminal offence referred to in Council Framework Decision 2002/584/JHA and

International conventions or treaties are agreements between countries that become legally binding agreements to the contracting States once they ratify them. One such legal instrument is the UN Convention on the Rights of the Child (UN CRC), which outlines the fundamental rights of every child, regardless of their race, religion, or abilities (UNICEF n.d.). As of 2024, 197 countries, including all EU member states, are parties to it.

Council of Europe Treaties, formally known as conventions, are legally binding international instruments that form the European legal space. The ratification of the convention by a member state creates an obligation in international law to implement it and comply with it (Council of Europe n.d.). Such legal instruments are the Lanzarote Convention and the Budapest Convention, which provide benchmarks on substantive criminal laws for the protection of children from sexual abuse and exploitation in the online environment (Children's Rights Division of the Council of Europe 2019). The former was ratified by all EU member states, while the latter by all but one EU member states.

Several types of legal act are used by the EU to achieve the different goals set out in its treaties, of which regulations and directives are the central types of instrument. Regulations like the Digital Services Act are directly applicable across the EU (European Union n.d.). Directives, like Directive 2011/93/EU, are also legally binding instruments but have to be transposed into national legislation (EU Monitor n.d.). In the following sections, we select some of the documents mentioned and analyze their relevance in seeking answers to the research questions. By evaluating these treaties, conventions, directives, and regulations, the manuscript critically assesses the adequacy of current legal frameworks in tackling both realistic and AI-driven CSAM, identifying potential gaps, and recommending necessary updates to address these emerging threats.

The following research questions aim to guide a comprehensive and systematic evaluation of European legislative measures:

> RQ1: Applicability to Virtual CSAM: How applicable are current legislative measures in addressing realistic CSAM images that depict virtual children and AI-driven CSAM (deepfakes), and what are the potential gaps?
>
> RQ2: Policy Recommendations: What policy recommendations can be made to address identified gaps in the European legislative framework concerning realistic CSAM, particularly those generated by AI technologies?

2.1. UN Convention on the Rights of the Child (1990)

The UN Convention on the Rights of the Child (UN CRC), adopted in 1990, is the first comprehensive international treaty that explicitly addresses and combats the sexual exploitation of children, establishing a legal framework for protecting children from all forms of sexual abuse and exploitation and obliging state parties to take legislative, administrative, and educational measures to safeguard children's rights. As such, it serves to set the guiding principle of the child rights-based approach in the pursuit of child protection (Goldhagen et al. 2020; Sandberg 2018). The UN CRC influenced directives such as the European Directive 2011/93/EU and Council of Europe conventions like the Lanzarote Convention (discussed below). It defines a child as "every human below the age of eighteen years unless, under the law applicable to the child, the majority is attained earlier" (United Nations 1990, Art. 1), and EU legislation use this definition and approach wherever they aim to provide legal protections to children. The UN CRC stipulates that in all actions concerning child victims of sexual violence, exploitation and abuse, whether undertaken in drafting laws, or by public or private social welfare institutions, police, courts of law, administrative authorities, or legislative bodies, the best interest of the child has to be a primary consideration (United Nations 2019, p. 17). The CRC's Optional Protocols, notably

punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years. Section 2(2) of the referred Council Framework Decision, among others, mentions the sexual exploitation of children and child pornography, giving relevance to the AIA with respect to the fight against online child sexual abuse.

the Protocol on the sale of children, child prostitution, and child pornography (OHCHR 2000), provide further important guidance for the realisation of children's rights concerning sexual exploitation and abuse online. It calls for legislative, policy, and educational initiatives guided by the best interest of the child, ensuring that European legal regulations are anchored in international child rights standards. This interaction ensures that EU legislative efforts to combat CSAM are child-centered, comprehensive, and aligned with global human rights standards. It is worth noting that the CRC does not specifically call for the criminalisation of child sexual abuse images, nor would it be a binding legal document for signing parties even if it did.

Similarly, the "Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents" (Rio Declaration, UNICEF 2008) is also a non-binding, international standard aimed at protecting children from online sexual exploitation. It calls on countries to continue to ratify and implement international human and child rights instruments, define, prohibit, and criminalise all acts of sexual exploitation of children in their justification, and establish effective extraterritorial jurisdiction. It also calls on countries to increase efforts to address the sexual exploitation of children and adolescents through the development of holistic national protection systems that aim to protect children from all forms of violence and exploitation.

2.2. Cybercrime Convention (2001)

The Council of Europe Convention on Cybercrime[8] requires ratifying states to criminalise offences against, and committed by, using computer systems, including child pornography (Art. 9), and provides law enforcement with effective means to investigate cybercrime and secure electronic evidence. It also establishes a framework for international police and judicial co-operation in computer-related cases involving crimes against children. Although it does lay down the foundations of co-operation between internet service providers (ISPs) and law enforcement, the Convention faces several challenges in prosecuting online CSAM in practice. These challenges are complex and involve both legal and technical aspects, and international co-operation.

The first challenge is the cross-border nature of cybercrime and CSAM, respectively. The internet's borderless nature complicates jurisdictional authority. Crimes involving CSAM often span multiple countries, each with its own legal framework and enforcement capabilities. Co-ordinating legal actions across jurisdictions can be challenging and time-consuming. The second issue is that ratifying countries may have inconsistent legal definitions of CSAM. Although the Council of Europe's Lanzarote Convention (Council of Europe 2007) and EU Directive 2011 against online child sexual abuse (which we address later) give unified definitions of CSAM ("child pornography"), different countries may have varying definitions of what constitutes CSAM, which can hinder mutual legal assistance and co-operation. For instance, what is considered illegal material in one country might not be illegal in another, leading to difficulties in prosecution and enforcement. Several authors emphasize that, in order to prosecute and investigate online child sexual abuse across national borders, countries rely heavily on extraterritorial jurisdiction clauses as well as informal and formal law enforcement collaboration channels (Broadhurst 2019; Witting 2021; Zharova 2023; Sorbán 2024). Thirdly, the variation in data retention laws across countries can affect the availability of crucial evidence. Some countries may have stringent data protection regulations that limit access to necessary data for investigations (Kasper and Laurits 2016). And, last but not least, obtaining digital evidence from ISPs and tech companies can be challenging, especially when these entities are based in different jurisdictions. Legal processes to access these data can be slow and bureaucratic (Atrey 2023).

[8] ETS No. 185, also known as the Budapest Convention, available online: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed on 25 October 2024).

2.3. The Lanzarote Convention (2007)

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (known as Council of Europe Treaty Series No. 201 or the Lanzarote Convention 2007) is the first convention to go beyond the possession, production, and dissemination of CSAM by identifying as an offence the solicitation of children for sexual purposes through computer systems, including child pornography, also known as "grooming". According to the Lanzarote Convention, both national and international co-operation are required from ratifying states for the effective eradication of online sexual exploitation and abuse of children and the protection of victims. The Budapest and Lanzarote Conventions combined contain a comprehensive set of measures that support the facilitation of international operational cooperation.

Third countries can accede to Council of Europe conventions, such as the Budapest and the Lanzarote Conventions, but they will only be binding for adopting countries if they also ratify them. Nevertheless, the lack of ratification or a failure to meet obligations arising from ratification will not entail sanctions against non-compliant states as the Council does not have an enforcement system (EFF n.d.). After ratification, states are obliged to transpose the treaty's recommendations into national legislation. Within the EU, directives are substantive legal instruments which specifically require member states to criminalise acts stipulated in them (Bux and Maciejewski 2024). However, as opposed to regulations that are directly applied to member states, directives offer a framework and pose obligations to member states, to meet specific goals within the member states' own legislative and non-legislative systems. The European Directive on combating the sexual abuse and sexual exploitation of children, and child pornography (2011/93/EU), is one such instrument criminalising all forms of CSAM.

2.4. European Directive 2011/93/EU

The European Directive on combating sexual abuse, sexual exploitation of children, and child pornography is a regional, European document treating sexual exploitation and abuse online (2011/93/EU, hereinafter European Directive). The Directive reflects the goals of both the Budapest and Lanzarote Conventions (Postolache 2023) in that it calls for the criminalisation of CSAM offences ("child pornography") and the definition of a child (anyone not older than 18 years of age). It proposes that ratifying states should criminalise all forms of online child sexual abuse, including realistic images and pseudo-photographs. It also adopts the Lanzarote Convention's proposal for criminalising online grooming with the intention of establishing physical contact with the child without the requirement of actual physical contact. To improve effectiveness, the directive introduces new provisions, which require authorities to adopt a more proactive approach to the detection of crimes. One such provision is that victims do not need to have submitted a complaint for the authorities to investigate and prosecute. Similarly, statutes of limitation applicable to the crimes must be extended to enable prosecution even after more than 18 years after the fact (Art. 15(2)) and investigative tools must be made available (Art. 15(3)). The European Directive seeks to lift existing barriers and demands the lifting of professional or medical confidentiality so that suspected sexual offences can be reported (Art. 16). To broaden the territorial scope of investigations, the European Directive demands the adoption of a clause of extraterritorial jurisdiction enabling authorities to pursue suspects including habitual residents who perpetrate offences in a third country (Art. 17). In support of a child-centered approach, member states are required to plan assistance, support and protection measures for victims from an early stage (Art. 18).

The European Directive is a binding legal document for member states of the European Union, which have to amend their regulations on online CSAM accordingly. It is a substantive criminal law instrument that requires member states to criminalise a series of offences and sets standards for prevention measures and victim support. However, its applicability in practice faces several challenges, and has received criticism. One of the primary concerns of its critics is its inconsistent implementation across EU member states. The Directive

gives broad discretion to member states in transposing its provisions. It contains minimum harmonization provisions, which oblige member states to criminalise certain acts and adopt certain levels of sanctions, but it also has numerous openly worded provisions. As a result, member states can interpret and enforce discretionary rules of the European Directive differently, leading to uneven levels of protection and enforcement. This variability can undermine the Directive's effectiveness in providing uniform safeguards for children across the EU (Huemer 2024).

Furthermore, resources and infrastructure available in member states for the effective implementation of the Directive vary significantly. Countries with more limited resources may struggle to meet the Directive's requirements, which causes gaps in protection and enforcement (Huemer 2024). The Directive mandates EU member states to criminalise and actively combat all forms of CSAM, implement victim support systems, conduct thorough investigations, and ensure cross-border cooperation. However, countries with limited resources may lack the necessary infrastructure, such as trained law enforcement personnel (Odink 2024), advanced technology for identifying CSAM (Henseler and de Wolf 2019; Steel 2024), and sufficient social services for victims (Joleby et al. 2021). This can lead to inconsistent enforcement of the Directive's provisions, creating gaps in protection where children are more vulnerable, and challenges in prosecution (van den Brink et al. 2022), particularly in less resourceful states. These gaps can also undermine broader European efforts to create uniform standards of child protection across the EU, and implement cross-border co-operation in Europol-led investigations or share critical intelligence with other EU member states (Broadhurst 2019).

Technical and legal challenges arise because of the European Directive's reliance on existing national legal frameworks and the resulting fragmentation of and significant differences in legal definitions and sanctions related to child sexual abuse and exploitation. This fragmentation complicates cross-border cooperation and enforcement (Huemer 2024). Rapid technological advancements also represent a challenge as they make implementing the European Directive difficult for law enforcement agencies. Experts say that the Directive needs continuous updates to address new forms of online child exploitation effectively (Huemer 2024). Due to the ongoing technological evolution of online CSAM, the European Directive does not cover all of the related technological issues, nor does it provide clues on how to reconcile respect for fundamental rights with the urgent need to combat the sexual abuse of children. Among other shortcomings, it does not provide guidelines on the realistic depiction of children or adults portraying children—which can include users' virtual alter egos or avatars on virtual reality platforms—or whether they should be criminalised, and it does not stipulate what measures should be implemented to enforce a takedown and to investigate such cases. Even in more regular cases, the detection of online CSAM is rendered difficult by end-to-end encrypted (E2EE) communications or by the anonymity of internet users.

The Directive also includes "realistic images of children" among the subjects of "child pornography" (the name of CSAM in the Directive), but it allows member states to deviate from this particular point and only criminalise depictions of real and existing children (Art. 2(c)). This results in discrepancies between states and has made co-operation difficult (Europol 2020a, 2020b). Regarding online CSAM, the case law of the European Courts of Human Rights (ECHR) could give some guidance on interpretation. However, even though the obligation of the members states to conduct effective criminal investigations in cases involving violence against children has been highlighted as a positive development in several cases, there is no case law at the moment that would address the realistic depiction of children in CSAM (Huemer 2024).

In addition, the European Directive mandates measures that are, at times, in conflict with stringent data protection laws, such as the General Data Protection Regulation of the European Union (GDPR). Balancing the need for privacy with the effective monitoring and enforcement against the exploitation of children remains a significant challenge (Internet Watch Foundation 2023), and we will discuss it further in the next section on the COM (2022)

209 Final. Furthermore, the effective implementation of the Directive requires effective co-ordination between various stakeholders, including law enforcement, child protection services, and non-governmental organisations. The lack of streamlined co-ordination mechanisms can hinder the Directive's effectiveness (Baines 2021), therefore, ensuring efficient cross-border co-operation among EU member states is crucial for addressing child exploitation. Due to differences between legal systems and enforcement capabilities, it remains a complex task, however (Baines 2021). A recent European Parliamentary Research Service (EPRS) analysis concluded that it is necessary to amend the Directive focusing on stronger preventive measures, educational programs, and assistance to victims, and more efficient investigation and prosecution mechanisms through international co-operation (Huemer 2024).

2.5. COM (2022) 209 Final

One of the latest initiatives in the fight against online CSAM is the EU Strategy for a More Effective Fight Against Child Sexual Abuse (European Commission 2020) published by the European Commission in 2020. An interim, temporary regulation was also proposed, which allows ISPs to derogate from the confidentiality requirement of the e-Privacy Directive[9]. This means that ISPs can scan user communications and report CSAM exchanges to LEAs on a voluntary basis. At the same time, this legislation did not constitute a legal basis for processing data and has created inefficiencies in the co-operation between public authorities and service providers (Rezende 2024). Given the expiration of the temporary interim regulation in August 2024, the European Commission extended this instrument referring to the COM (2022) 209 Final (hereinafter Proposed Regulation). Compliance with the Proposed Regulation is not voluntary, and it imposes obligations on ISPs to detect, report, and remove CSAM on their platforms. The Proposed Regulation seems appropriate and timely (Tolbaru 2022), but it also drew significant criticism (Rezende 2024). First of all, it is criticized by privacy experts and data protection authorities for mandating ISPs to monitor user communications and empowering LEAs to widely decrypt users' communications contents (E2EE), practices considered disproportionate in democratic societies (Koops and Kosta 2018; Oerlemans and Galič 2022; *Open Letter* 2023). Secondly, the absence of common standards of admissibility of evidence in the EU and the limited relevance of privacy considerations in defining such standards (European Law Institute 2023, p. 14) have the result that data gathered through ISP-executed surveillance (monitoring) could jeopardize individuals' rights in criminal proceedings. This issue arises in complex, multi-level legal frameworks like the EU with several different criminal procedure systems, which are only bound by minimal fair trial standards at the European level (Claverie-Rousset 2013; Ligeti et al. 2020; Bachmaier 2023).

The Proposed Regulation establishes the European Union Agency to Prevent and Combat Child Sexual Abuse (the EU Centre), which will create and maintain databases of known CSAM and develop "indicators" to detect new CSAM and grooming material online. However, to detect new CSAM, detection orders must be issued that are in conflict with the confidentiality requirements of the e-privacy Directive of the EU. However, because detection orders targeting the solicitation of children are allowed only if children are involved in the communication, all users will have to submit their data to age verification systems. Such tools interfere with the right to private life as they rely on biometric processing or extensive profiling. For example, social media companies like Instagram are currently testing AI-powered solutions with which users can verify their age. Such a solution is, for instance, Yoti, a platform which estimates people's age by scanning their faces (Postolache 2023). Another method to verify the age of users is requiring new users to send a selfie video to Yoti, which, in turn, uses machine learning to estimate the user's age. Since 2021, Instagram has been using automatic systems to identify underage users. These tools scan

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) OJ L 201, 31 July 2002.

user information such as birthday posts and the average age of their friends to identify user age (Postolache 2023). A verification system is most certainly needed to identify previously unknown CSAM, as well as its distribution pathways.

Artificial intelligence can now be used for facial and voice recognition (biometrics) in automated searches. Biometrics can aid in determining whether CSAM is new, previously known, or irrelevant. Information from various different sources of imagery (videos and still images) can be used to compile a more accurate profile (Westlake 2020). Critics say, however, that introducing such automated age verification/monitoring systems would eventually have a chilling effect on the use of interpersonal communications services (van Daalen 2023). Individuals might refrain from using communication platforms or services, fearing that their privacy could be compromised or that their interactions are being monitored, even when not engaging in illegal or harmful activities. If ISPs are pressured to implement automated monitoring, it could conflict with the privacy guarantees offered by E2EE, reducing privacy protections for all users and possibly hindering free online communication. This self-censorship can curb freedom of expression and would discourage or even prevent the use of E2EE by ISPs.

According to critics, technologies used for detecting CSAM and grooming are considered incompatible with E2EE (Draper 2022, p. 28; *Open Letter* 2023). The Regulation also indirectly overloads Europol with CSAM filtering requirements, which would inevitably lead to many false positives on account of the fact that detection tools process content communications automatically and typically rely on AI. Such technologies used to detect grooming have inherently high error rates (European Parliamentary Research Service 2021, p. 16) and can be easily circumvented (European Parliamentary Research Service 2023, p. 17). Reports following a detection order may include all content data, including images, videos, and text and all available data other than context data (COM (2022) 209 Final Art. 13c and d). This may easily overload Europol with filtering tasks, as large quantities of unnecessary data would end up in its databases, including personal details (names, surnames) and financial and behavioral data that might allow the profiling of individuals whose link to child sexual abuse offences has not been identified yet. It is also unclear how national LEAs could repurpose these data in other investigations since there is little guidance and no common rules on the admissibility of evidence at EU level (Ligeti et al. 2020; Bachmaier 2023), which could significantly affect individuals' rights.

Furthermore, while child sexual abuse is a heinous crime, it does not raise national security issues; the only occasion the CJEU justifies measures that counteract the proportionality rule within the EU (CJEU Privacy International § 75[10]; CJEU GD § 57[11]). Lastly, the Regulation does not address the consensual exchange of self-generated content between minors. The Lanzarote Convention's evaluation committee (Lanzarote Committee 2022, p. 26) identifies the decriminalisation of consensual sexual activities between children who have reached the legal age of sexual activities as a promising practice as this is increasingly considered normal by adolescents (Madigan et al. 2018a, 2018b; Needham 2021). However, materials exchanged between consensual adolescents (minors) may also be flagged as CSAM by automated detecting technologies (Witting and Leiser 2022, p. 31). This could impact children's rights to privacy disproportionately and lead to undue criminalisation and stigmatisation.

2.6. The Digital Services Act (DSA 2022)

Artificial intelligence (AI) plays an increasingly significant role in generating harmful online material, which represents a challenge for legislators. Mania (2024) for example reveals in a comparative legal study that EU member states adopted different legislations to regulate and prosecute AI-driven content. Mania (2024) describes the legislative initia-

[10] Privacy International v Secretary of State for Foreign and Commonwealth Affairs and o., Case C-623/17, 6.10.2020.

[11] GD v Commissioner of An Garda Síochána and o., Case C-140/20, 5.04.2022.

tives of EU member states on deepfake and revenge porn material as diverse and often unrealistic. She defines deepfake and revenge porn as the non-consensual dissemination of intimate images, often with the help of AI technology (Mania 2024, p. 119). One of the challenges in prosecuting such material is rooted in the autonomy of national legislatures and the resulting significant differences between the member states of the EU. Although the GDPR leaves decisions on the enforcement of privacy and personal data disputes with the individuals concerned, this has not proved effective for victims of revenge and deepfake porn. The onus of pursuing their private images online, contacting the ISPs, and convincing them to remove the images is on users. The removal process is time-consuming and costly, discouraging victims from coming forward and asserting their rights.

The right to erasure is difficult to assert and does not necessarily achieve the desired success (Politou et al. 2018). Moreover, the data subject to removal are often stored in a country different from the country of prosecution, and victims often face problems with law enforcement jurisdiction as a result (Tesfay et al. 2018). The Digital Services Act (DSA 2022) entered into effect on 17 February 2024, bringing some much-needed order into the process of remedying individual rights. The DSA regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms with the goal of preventing illegal and harmful activities and the spread of disinformation online. It ensures user safety, protects fundamental rights and creates a fair and open online platform environment by imposing obligations and responsibilities on intermediaries in the single market across borders, regardless of users' place of residence within the EU. It provides the appropriate protection of user rights and children online by requiring online platforms, hosting services—such as cloud and web hosting services—and intermediary services offering network infrastructure to remove illegal online content, including CSAM within a short time (Heldt 2022; Wilman 2022). This immediate takedown mechanism ensures that harmful content is quickly removed, which protects children from continued exploitation. In addition, very large online platforms (VLOPs)—defined as those with over 45 million monthly active users—are required to conduct annual risk assessments. These assessments evaluate the potential negative impacts on users, including children, and ensure that platforms take steps to mitigate these risks, such as improving privacy settings and moderating harmful content more effectively (Frosio and Geiger 2023; World Economic Forum 2022).

The DSA also includes a complete ban on targeted advertising aimed at minors based on profiling or personal data. It establishes a robust framework for monitoring and enforcing compliance. In collaboration with the European Commission, national authorities will ensure that platforms adhere to the new regulations (Heldt 2022; Wilman 2022). This includes setting up an advisory body overseeing the consistent application of the rules across the EU. Who has responsibility for investigating and prosecuting illegal and harmful material will still depend on the member states, however, as criminal law falls under their own sovereign regulation (Bachmaier 2023). Cauffman and Goanta (2021) further state that the instruments of the DSA are limited procedurally since they do not sufficiently incorporate procedures for dealing with illegal content after removal (see also Turillazzi et al. 2023).

3. Conclusions

Given the extensive harm caused by CSAM—ranging from the ongoing psychological trauma inflicted on its victims (Gewirtz-Meydan et al. 2018, 2019; Svedin and Back 2003) to the potential for normalizing risky sexual behavior (Foothills Child Advocacy Centre n.d.; Taylor 2018) and escalating sexual violence (Diamond et al. 2011)—criminalising AI-driven CSAM is imperative. Despite no physical abuse being involved, AI-driven content perpetuates the same cycles of victimisation, desensitises offenders (Seigfried-Spellar and Rogers 2013), fuels harmful fantasies, hinders the identification of real victims, which may increase the risk of contact offences (van Es 2016; Insoll et al. 2022; Johnson 2020), and place

a significant burden on law enforcement (Krishna et al. 2024; NCMEC 2024). Therefore, societal and individual harms caused by virtual CSAM justify its criminalisation.

RQ1: Applicability to Virtual CSAM: How applicable are current legislative measures in addressing realistic CSAM images that depict virtual children, and AI-generated or manipulated CSAM (deepfakes), and what are the potential gaps?

Although the EU's legislative instruments have created a legal basis for recognizing, investigating, and prosecuting realistic and AI-generated or manipulated CSAM, there still remain some important concerns. First, although the EU's legislative instruments define CSAM ("child pornography") as depictions of real children and also realistic depictions of children (Cybercrime Convention, Lanzarote Convention, EU Directive 2011/93/EU), the latter rule allows for exceptions. As a result, member states are still allowed to only criminalise CSAM that depict real children without the criminalisation of AI-generated or manipulated (deepfake) CSAM. However, given the rapid technological development that enables everyone to utilize AI technology to create or manipulate existing CSAM, it is inevitable that AI-driven CSAM will flood the internet, and addressing that will require concerted efforts from LEAs, ISPs, and other stakeholders in the fight against CSAM. Research posits that realistic and deepfake CSAM can be equally harmful to children, can lead to online habituation (Cummins 2007; Linz and Imrich 2001), online disinhibition (Suler 2004), and can be easily connected to offline or "contact" offences involving real children (Seto et al. 2001; Sullivan and Sheehan 2016; Seto and Eke 2005), although research on causality is inconclusive. In addition, online CSAM does not respect borders, and all CSAM-related acts, including the possession, creation, distribution, and sharing of CSAM, infringe on the rights of the child, which means that even virtual CSAM images harm children in general. It is, therefore, a societal responsibility to adopt legal regulations of the highest possible standard, which enable the prosecution and cross-border co-operation in CSAM cases.

This brings us to the next point: cross-border co-operation. Although the Cybercrime Convention lays down the requirements for data preservation, disclosure, collection, and interception, data acquisition from ISPs can be difficult due to conflicts between security and privacy rights and regulations. The variation in data retention laws across countries can affect the availability of crucial evidence. Some countries may have stringent data protection regulations that limit access to necessary data for investigations. The Cybercrime Convention also sets general rules for cross-border co-operation, but jurisdictional issues can hamper obtaining digital evidence and render cooperation inefficient (Sorbán 2024). Legal processes to access these data can be slow and bureaucratic.

RQ2: Policy Recommendations: What policy recommendations can be made to address identified gaps in the EU's legislative framework concerning realistic CSAM, particularly those generated by AI technologies?

The definition and scope of online CSAM must be standardized to avoid discrepancies in national and international laws. Member states must implement EU legal standards to the greatest possible extent that allows them to criminalise offences involving realistic and AI-generated or manipulated (deepfake) CSAM.

Many children use "avatars" or pseudonyms today to protect their identity on virtual platforms. This means that children are potentially present with a fake identity and are subject to victimisation without adequate safeguard mechanisms (Lin and Latoschik 2022). Adult users can also become a victim of online harassment and sextortion on virtual reality platforms such as Meta (Blackwell et al. 2019; Robinson et al. 2020). Online platforms should, therefore, not only use age verification systems that block minor users from accessing their platforms more efficiently but also offer community guidelines and support systems for adult users who are targeted or victimized (Chawki et al. 2024).

The rapid evolution of technology means that new methods of committing and concealing crimes are constantly emerging. Law enforcement agencies must continuously update their skills and tools to keep up with these changes, with the support of national, EU, and international institutions such as Europol and Interpol.

Investigating and prosecuting CSAM requires significant resources, including specialized training for law enforcement officers and advanced technological tools. Many countries, especially developing ones, lack these resources, which hampers effective enforcement, evidence gathering, and co-operation with other states' LEAs. Qin et al. (2022), therefore, recommend creating an international legal framework to enhance global collaboration.

The variation in data retention laws across countries can affect the availability of crucial evidence. Some countries may have stringent data protection regulations that limit access to necessary data for investigations. To resolve this, the data retention laws of member states must be standardized to achieve the greatest possible success in digital evidence acquisition.

The absence of harmonized cybercrime laws across countries can impede international co-operation. The Cybercrime Convention provides a framework, but not all countries are signatories, and those that are may implement its provisions differently. International co-operation can be slow and inefficient, delaying critical actions needed to prevent ongoing abuse and secure evidence for prosecution. Recent UN negotiations for creating a global cybercrime convention are ongoing (UNODC n.d.). The UN's global convention aims to address the growing global threat of cybercrime through a comprehensive and legally binding framework. Ongoing discussions also emphasize the importance of global co-operation and effective safeguards against the potential misuse of constantly developing surveillance tools such as AI (Lindsey and Pavlova 2024; Kazakova 2024).

In order to achieve a balance between users' rights, platform accountability, and the demands of technological advancements, co-operation between sectors must be enhanced. For example, WePROTECT, a "Global Alliance to End Child Sexual Exploitation Online", which involves technology companies, international organisations, and countries, is a good example of a multi-stakeholder, co-ordinated approach to tackle the threat that has no borders in the Metaverse (Pardhey et al. 2024). Such cross-border alliances of public and private agencies like AI system developers, ISPs, and LEAs, could resolve the problems of non-co-operation and non-compliance.

Author Contributions: Conceptualization, K.P.; methodology, K.P.; software, K.P.; validation, K.P., and J.S.; formal analysis, K.P. and J.S.; investigation, K.P and J.S.; resources, K.P.; data curation, K.P.; writing—original draft preparation, K.P.; writing—review and editing, K.P. and J.S.; supervision, K.P.; project administration, K.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article. The original contributions presented in the study are included in the article; further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

Ali, Sana, Saadia Anwar Pasha, Ann Cox, and Enaam Yousseff. 2024. Examining the short and long-term impacts of child sexual abuse: A review study. *SN Social Sciences* 4: 1–15. [CrossRef]

Atrey, Ishan. 2023. Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews* 10: 183–97.

Bachmaier, Lorena. 2023. Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings? *Eucrim* 2: 223–29. [CrossRef]

Baines, Victoria. 2021. Member State Responses to Prevent and Combat Online Child Sexual Exploitation and Abuse. Council of Europe. Available online: https://rm.coe.int/191120-baseline-mapping-web-version-3-/168098e109 (accessed on 15 July 2024).

Bendiek, Annegret, and Eva Pander Maat. 2019. The EU's Regulatory Approach to Cybersecurity. Available online: https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf (accessed on 15 July 2024).
Blackwell, Lindsay, Nicole Ellison, Natasha Elliott-Deflo, and Raz Schwartz. 2019. Harassment in social virtual reality: Challenges for platform governance. *Proceedings of the ACM on Human-Computer Interaction* 3: 1–25. [CrossRef]
Broadhurst, Roderick. 2019. Child Sex Abuse Images and Exploitation Materials. In *The Human Factor of Cybercrime*. Edited by Rutger Leukfeldt and Thomas J. Holt. London: Routledge, pp. 310–36. [CrossRef]
Bux, Udo, and Mariusz Maciejewski. 2024. Sources and Scope of European Union Law. Fact Sheets on the European Union. Available online: https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law (accessed on 16 July 2024).
Canadian Centre for Child Protection. 2017. Survivor's Survey. Executive Summary. Available online: https://content.c3p.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf (accessed on 15 July 2024).
Carrera, Sergio, and Elspeth Guild. 2014. The European Council's guidelines for the Area of Freedom, Security and Justice 2020: Subverting the 'Lisbonisation' of Justice and Home Affairs? Available online: https://ssrn.com/abstract=2476887 (accessed on 15 July 2024).
Cauffman, Caroline, and Catalina Goanta. 2021. A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation* 12: 758–74. [CrossRef]
Chawki, Mohamed, Subhajit Basu, and Kyung-Shick Choi. 2024. Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws* 13: 33. [CrossRef]
Children's Rights Division of the Council of Europe. 2019. Comments submitted by the Children's Rights Division of the Council of Europeon the UN Committee on the Rights of the Child Concept Note for a General Comment on Children's Rights to Access to Justice and Effective Remedies. Available online: https://www.ohchr.org/sites/default/files/documents/hrbodies/crc/gcomments/gc27/cfi/subm-general-comment-regi-orga-unit-nati-agen-mech-council-europe-children-rights-div-ision.docx (accessed on 15 July 2024).
Claverie-Rousset, Charlotte. 2013. The admissibility of evidence in criminal proceedings between European Union Member States. *European Criminal Law Review* 3: 152–69. [CrossRef]
Council of Europe. 2007. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201). Available online: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201 (accessed on 15 July 2024).
Council of Europe. n.d. Conventions and Treaties—Where Do They Come From? Available online: https://www.coe.int/t/dg3/children/keyLegalTexts/conventionsandTreatiesBackground_en.asp (accessed on 15 July 2024).
Cummins, R. Glenn. 2007. Pornography, x-rated movies. In *Encyclopedia of Children, Adolescents, and the Media*. Edited by Jeffrey Jensen Arnett. Thousand Oaks, CA: Sage, vol. 2, pp. 666–68.
Diamond, Milton, Eva Jozifkova, and Petr Weiss. 2011. Pornography and Sex Crimes in the Czech Republic. *Archives of Sexual Behavior* 40: 1037–43. [CrossRef]
Draper, Laura. 2022. Protecting children in the age of end-to-end encryption. *Joint PIJIP/TLS Research Paper Series* 80. Available online: https://digitalcommons.wcl.american.edu/research/80 (accessed on 20 June 2024).
ECPAT. 2016. Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Adopted by the Interagency Working Group on Sexual Exploitation of Children. Available online: https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf (accessed on 15 July 2024).
Electronic Frontier Foundation (EFF). n.d. Council of Europe. Available online: https://www.eff.org/issues/council-europe (accessed on 20 June 2024).
Endrass, Jérome, and Astrid Rossegger. 2010. Child Pornography as a Risk Factor for Hands-on Sex-offending? *European Psychiatry* 25: 676. [CrossRef]
EU Monitor. n.d. Directive. Available online: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vh7bhovywnh7 (accessed on 15 July 2024).
European Commission. 2020. EU Strategy for a More Effective Fight Against Child Sexual Abuse. Available online: https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en (accessed on 15 July 2024).
European Commission. 2022. New EU Strategy to Protect and Empower Children in the Online World. Press Release. Available online: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2825 (accessed on 25 June 2024).
European Commission. 2024. European Union Internet Forum. Available online: https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en (accessed on 10 July 2024).
European Law Institute. 2023. ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. Draft Legislative Proposal. Available online: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf (accessed on 11 July 2024).

European Parliamentary Research Service. 2021. Commission Proposal on the Temporary Derogation from the e-Privacy Directive for the Purpose of Fighting Online Child Sexual Abuse. Available online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662598 (accessed on 25 June 2024).
European Parliamentary Research Service. 2023. Proposal for a Regulation Laying Down the Rules to Prevent and Combat Child Sexual Abuse: Complimentary Impact Assessment. Available online: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf (accessed on 25 June 2024).
European Union. n.d. Types of Legislation. Available online: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en (accessed on 15 July 2024).
Europol. 2020a. Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic. Available online: https://www.europol.europa.eu/cms/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf (accessed on 11 July 2024).
Europol. 2020b. Internet Organised Crime Threat Assessment (IOCTA) 2020. Available online: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (accessed on 15 July 2024).
Foothills Child Advocacy Centre. n.d. The Impact of Child Pornography on Victims. Available online: https://www.foothillscac.org/uploads/9/9/2/1/9921414/the_impact_of_child_pornography_on_victims.pdf (accessed on 15 July 2024).
Frosio, Giancarlo, and Christophe Geiger. 2023. Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal* 29: 31–77. [CrossRef]
Fuster, Gloria González, and Lina Jasmontaite. 2020. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In *The Ethics of Cybersecurity*. Edited by Marcus Christen, Bert Gordijn and Michele Loi. Berlin and Heidelberg: Springer Nature, pp. 97–115. [CrossRef]
Gewirtz-Meydan, Alteret, Wendy Walsh, Janis Wolak, and David Finkelhor. 2018. The complex experience of child pornography survivors. *Child Abuse and Neglect* 80: 238–48. [CrossRef] [PubMed]
Gewirtz-Meydan, Alteret, Yael Lahav, Wendy Walsh, and David Finkelhor. 2019. Psychopathology among adult survivors of child pornography. *Child Abuse and Neglect* 98: 104189. [CrossRef] [PubMed]
Goldhagen, Jeffrey, Andrew Clarke, Peter Dixon, Anna Isabel Guerreiro, Garrison Lansdown, and Ziba Vaghri. 2020. Thirtieth anniversary of the UN Convention on the Rights of the Child: Advancing a child rights-based approach to child health and well-being. *BMJ Paediatrics Open* 4: e000589. [CrossRef] [PubMed]
Heldt, Amélie P. 2022. EU Digital Services Act: The White Hope of Intermediary Regulation. Digital Platform Regulation. In *Digital Platform Regulation. Palgrave Global Media Policy and Business*. Edited by Terry Flew and Fiona R. Martin. Cham: Palgrave Macmillan, pp. 69–84. [CrossRef]
Henseler, Hans, and Rens de Wolf. 2019. Sweetie 2.0 Technology: Technical Challenges of Making the Sweetie 2.0 Chatbot. In *Sweetie 2.0: Using Artificial Intelligence To Fight Webcam Child Sex Tourism*. Edited by Simone van der Hof, Ilina Georgieva, Bart Schermer and Bert-Jaap Koops. The Hague: T.M.C. Asser Press, pp. 113–134. [CrossRef]
Hörnle, Tatjana, Carina Tetal, and Gunda Wössner. 2024. Reoffending after convictions related to child sexual exploitation material: Data from the German Federal Central Criminal Register. *Child Abuse and Neglect* 153: 106806. [CrossRef]
Huemer, Marie-Astrid. 2024. Revision of Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography. Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757790/EPRS_BRI(2024)757790_EN.pdf (accessed on 25 June 2024).
Hunt, Philip, and Margaret Braid. 1990. Children of sex rings. *Child Welfare: Journal of Policy, Practice, and Program* 69: 195–207.
Insoll, Tegan, Anna Kateriina Ovaska, Juha Nurmi, Mikko Aaltonen, and Nina Vaaranen-Valkonen. 2022. Risk Factors for Child Sexual Abuse Material Users Contacting Children Online: Results of an Anonymous Multilingual Survey on the Dark Web. *Journal of Online Trust and Safety* 1: 1–24. [CrossRef]
Internet Watch Foundation. 2023. How AI Is Being Abused to Create Child Sexual Abuse Imagery. Available online: https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf (accessed on 11 July 2024).
Interpol. 2022. INTERPOL Secretary General: Online Child Sexual Abuse at Record Levels. Available online: https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-Secretary-General-Online-child-sexual-abuse-at-record-levels#:~:text=In%20a%20panel%20on%20cyber,the%20%20worst%20%20year%20on%20%20record (accessed on 11 July 2024).
Johnson, Scott A. 2020. Child porn users & risk for engaging in contact offenses: Faulty data minimizes offender's risk & puts more children at risk for sexual abuse. *Forensic Research and Criminology International Journal* 8: 93–99. [CrossRef]
Joleby, Malin, Sara Landström, Carolina Lunde, and Linda S. Jonsson. 2021. Experiences and Psychological Health among Children Exposed to Online Child Sexual Abuse—a Mixed Methods Study of Court Verdicts. *Psychology, Crime & Law* 27: 159–81. [CrossRef]
Kasper, Agnes, and Eneli Laurits. 2016. Challenges in collecting digital evidence: A legal perspective. In *The Future of Law and eTechnologies*. Edited by Tanel Kerikmäe and Addi Rull. Cham: Springer, pp. 195–233. [CrossRef]
Kazakova, Anastasiya. 2024. UN Cybercrime Convention: Will States Give in Disagreements for the Sake of a Global Common Threat? Available online: https://dig.watch/updates/un-cybercrime-convention-will-states-give-in-disagreements-for-the-sake-of-a-global-common-threat (accessed on 21 June 2024).
Kloess, Juliane A., Jessica Woodhams, Helen Whittle, Tim Grant, and Catherine E. Hamilton-Giachritsis. 2017. The challenges of identifying and classifying child sexual abuse material. *Sexual Abuse* 31: 173–96. [CrossRef]

Knack, Natasha, Dave Holmes, and J. Paul Fedoroff. 2020. Motivational pathways underlying the onset and maintenance of viewing child pornography on the Internet. *Behavioral Sciences and the Law* 38: 100–16. [CrossRef]
Koops, Bert-Jaap, and Eleni Kosta. 2018. Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "Going Dark". *Computer Law and Security Review* 34: 890–900. [CrossRef]
Korff, Douwe. 2019. First do no harm: The potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions. In *Research Handbook on Human Rights and Digital Technology*. Edited by Ben Wagner, Matthias C. Kettemann and Kilian Vieth. Cheltenham: Edward Elgar Publishing Limited, Northampton, MA: Edward Elgar Publishing, Inc., pp. 129–55. [CrossRef]
Krishna, Shruthi, Fiona Dubrosa, and Ruth Milanaik. 2024. Rising threats of AI-driven child sexual abuse material. *Pediatrics* 153: e2023063954. [CrossRef] [PubMed]
Krone, Tony, Russell G. Smith, Jenny Cartwright, Alice Hutchings, Adam Tomison, and Sarah Napier. 2017. Online Child Sexual Exploitation Offenders: A Study of Australian Law Enforcement Data. Available online: https://www.aic.gov.au/sites/default/files/2020-05/58-1213-FinalReport.pdf (accessed on 15 July 2024).
Lanzarote Committee. 2022. The Protection of Children against Sexual Exploitation and Sexual Abuse Facilitated by Information and Communication Technologies (ICTs): Addressing the Challenges Raised by Child Self-Generated Sexual Images and/or Videos. Available online: https://rm.coe.int/implementation-report-on-the-2nd-monitoring-round-the-protection-of-ch/1680a619c4 (accessed on 11 July 2024).
Ligeti, Katalin, Balázs Garamvölgyi, Anna Ondrejová, and Margarete von Galen. 2020. Admissibility of Evidence in Criminal Proceedings in the EU. *Eucrim* 3: 201–8. Available online: https://eucrim.eu/media/issue/pdf/eucrim_issue_2020-03.pdf#page=47 (accessed on 11 July 2024).
Lin, Jinghuai, and Marc Erich Latoschik. 2022. Digital body, identity and privacy in social virtual reality: A systematic review. *Frontiers in Virtual Reality* 3: 974652. [CrossRef]
Lindenhovius, Caitlin. 2022. Sexual exploitation of children: Protection from more than the public. *Liberty University Law Review* 16: 307–43.
Lindsey, Charlotta, and Pavlina Pavlova. 2024. UN Cybercrime Convention: Negotiators Request More Time as Consensus Remains Elusive. CyberPeace Institute. Available online: https://cyberpeaceinstitute.org/news/concluding-session-ahc/ (accessed on 5 June 2024).
Linz, Daniel, and Dorothy Imrich. 2001. Child Pornography. In *Handbook of Youth and Justice. The Plenum Series in Crime and Justice*. Edited by Susan O. White. Boston: Springer, pp. 79–111. [CrossRef]
Lovett, Samuel. 2024. 'Silent Epidemic' of Online Child Abuse Surging Follow Pandemic. *The Telegraph*. March 9. Available online: https://www.telegraph.co.uk/news/2024/03/09/silent-epidemic-online-child-abuse-surging-follow-pandemic/ (accessed on 11 July 2024).
Madigan, Sheri, Anh Ly, Christina L. Rash. Joris Van Ouytsel, and Jeff R. Temple. 2018a. Prevalence of multiple forms of sexting behavior among youth. *JAMA Pediatrics* 172: 327–35. [CrossRef]
Madigan, Sheri, Joris Van Ouytsel, and Jeff R. Temple. 2018b. Nonconsensual sexting and the role of sex differences—Reply. *JAMA Pediatrics* 172: 890–91. [CrossRef]
Mania, Karolina. 2024. Legal protection of revenge and deepfake porn victims in the European Union: Findings from a comparative legal study. *Trauma, Violence, and Abuse* 25: 117–29. [CrossRef]
Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul de Hert. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review* 35: 105336. [CrossRef]
Murphy, Colin. 2024. Understanding Cybercrime. Briefing: EU Policies—Insight. European Parliamentary Research Service. Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf (accessed on 21 June 2024).
National Centre for Missing & Exploited Children (NCMEC). 2021. CyberTipline 2021 Report. Available online: https://www.missingkids.org/content/dam/missingkids/pdfs/2021-CyberTipline-Report.pdf (accessed on 25 June 2024).
National Centre for Missing & Exploited Children (NCMEC). 2022. Be the Support. Helping Victims of Child Sexual Abuse Material: A Guide for Mental Health Professionals. Available online: https://www.missingkids.org/content/dam/missingkids/pdfs/be-the-support.pdf (accessed on 15 July 2024).
National Centre for Missing & Exploited Children (NCMEC). 2023. CyberTipline 2023 Report. Available online: https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf (accessed on 25 June 2024).
National Centre for Missing & Exploited Children (NCMEC). 2024. Generative AI CSAM Is CSAM. Available online: https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam (accessed on 15 July 2024).
Needham, Jon. 2021. Sending nudes: Intent and risk associated with 'sexting' as understood by gay adolescent boys. *Sexuality & Culture* 25: 396–416. [CrossRef]
Odink, Ingeborg. 2024. Combating Child Sexual Abuse. Revising Directive (2011/93/EU)—Recast. Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762374/EPRS_BRI(2024)762374_EN.pdf (accessed on 15 July 2024).
Oerlemans, Jan-Jaap, and Maša Galič. 2022. Cybercrime investigations. In *Essentials in Cybercrime. A Criminological Overview for Education and Practice*. Edited by Wytske van der Wagen, Jan-Jaap Oerlemans and Marleen Weulen Kranenbarg. The Hague: Eleven International Publishing, pp. 197–254.

OHCHR. 2000. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. Resolution A/RES/54/263 at the Fifty-Fourth Session of the General Assembly of the United Nations. Available online: https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child (accessed on 15 July 2024).

Okolie, Chidera. 2023. Artificial intelligence altered videos (deepfakes), image-based sexual abuse, and data privacy concerns. *Journal of International Women's Studies* 25: 1–17.

Open Letter from Security and Privacy Researchers in Relation to the Online Safety Bill. 2023. Available online: https://haddadi.github.io/UKOSBOpenletter.pdf (accessed on 5 June 2024).

Pardhey, Nanda, Rui Dias, Mohammad Irfan, Rosa Galvão, Miguel Varela, and Rui Ribeiro. 2024. Insight into child and youth safety online via international laws edges. *Revisita de Gestao Social e Ambiental* 18: 1–20. [CrossRef]

Pavlova, Pavlina. 2020. Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups. *Peace Human Rights Governance* 4: 391–418. [CrossRef]

Politou, Eugenia, Alexandra Michota, Efthimios Alepis, Matthias Pocs, and Constantinos Patsakis. 2018. Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review* 34: 1247–57.

Postolache, Mihaela. 2023. Trends regarding measures to combat sexual abuse of minors in the online environment. *Curentul Judiric* 95: 128–33.

Qin, Hua Xuan, Yuyang Wang, and Pan Hui. 2022. Identity, crimes, and law enforcement in the Metaverse. *arXiv* arXiv:2210.06134. [CrossRef]

Rezende, Izadora Neroni. 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 & Technology* 38: 369–90. [CrossRef]

Robinson, Laura, Jeremy Schulz, Grant Blank, Massimo Ragnedda, Hiroshi Ono, Bernie Hogan, Gustavo S. Mesch, Shelia R. Cotten, Susan B. Kretchmer, Timothy M. Hale, and et al. 2020. Digital inequalities 2.0: Legacy inequalities in the information age. *First Monday* 25: 1–27. [CrossRef]

Russell, Diana, and Natalie Purcell. 2008. Exposure to pornography as a cause of child sexual victimization. In *Handbook of Children, Culture, and Violence*. Edited by Nancy E. Dowd, Dorothy G. Singer and Robin Fretwell Wilson. New York: SAGE Publications, Inc., pp. 59–84. [CrossRef]

Sandberg, Kirsten. 2018. Children's Right to Protection Under the CRC. In *Human Rights in Child Protection*. Edited by Asgeir Falch-Eriksen and Elisabeth Backe-Hansen. Cham: Palgrave Macmillan, pp. 15–38. [CrossRef]

Seigfried-Spellar, Kathryn C., and Marcus Rogers. 2013. Does deviant pornography use follow a Guttman-like progression? *Computers in Human Behavior* 29: 1997–2003. [CrossRef]

Seto, Michael C., Alexandra Maric, and Howard E. Barbaree. 2001. The role of pornography in the etiology of sexual aggression. *Aggression and Violent Behavior* 6: 35–53. [CrossRef]

Seto, Michael C., and Angela W. Eke. 2005. The criminal histories and later offending of child pornography offenders. *Sexual Abuse* 17: 201–10. [CrossRef] [PubMed]

Shuck, Brad. 2011. Integrative Literature Review: Four Emerging Perspectives of Employee Engagement. *Human Resource Development Review* 10: 304–28. [CrossRef]

Silbert, Mimi Halper. 1989. The effects on juveniles of being used for prostitution and pornography, sexual assault of prostitutes. In *Pornography Research Advances and Policy Considerations*. Edited by Dolf Zillmann and Jennings Bryant. Mehwah, NJ: Lawrence Erlbaum Associates, Inc.

Sorbán, Kinga. 2024. Procedural dilemmas of cybercrimes involving illegal content dissemination in cross-border situations. *Belügyi Szemle* 72: 133–51. [CrossRef]

Steel, Chad M.S. 2024. Artificial Intelligence and CSEM—A Research Agenda. *Child Protection and Practice* 2: 100043. [CrossRef]

Suler, John. 2004. The Online Disinhibition Effect. *CyberPsychology & Behavior* 7: 321–26. [CrossRef]

Sullivan, Joe, and Valeria Sheehan. 2016. What motivates sexual abusers of children? A qualitative examination of the Spiral of Sexual Abuse. *Aggression and Violent Behavior* 30: 76–87. [CrossRef]

Svedin, Carl Göran, and Christina Back. 2003. *Why Didn't They Tell Us? On Sexual Abuse in Pornography*. Stockholm: Save the Children Sweden. Available online: https://resourcecentre.savethechildren.net/document/why-didnt-they-tell-us-sexual-abuse-child-pornography/ (accessed on 10 July 2024).

Taylor, Elisabeth. 2018. Pornography as a public health issue: Promoting violence and exploitation of children, youth, and adults. *Dignity: A Journal on Sexual Exploitation and Violence* 3: 8. [CrossRef]

Tesfay, Welderufael B., Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, and Jetzabel Serna. 2018. PrivacyGuide: Towards an implementation of the EU GDPR on internet privacy policy evaluation. Paper presented at the Fourth ACM International Workshop on Security and Privacy Analytics, Tempe, AZ, USA, March 21.

The Crown Prosecution Service. 2018. Indecent and Prohibited Images of Children. Available online: https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children (accessed on 15 July 2024).

Thiel, David, Melissa Stroebel, and Rebecca Portnoff. 2023. Generative ML and CSAM: Implications and Mitigations. Available online: https://stacks.stanford.edu/file/druid:jv206yg3793/20230624-sio-cg-csam-report.pdf (accessed on 11 July 2024).

Tolbaru, Carmina-Elena. 2022. Fight against sexual abuse and online exploitation of children–key priority at the European Union level. *International Journal of Legal and Social Order* 1: 347–56. [CrossRef]

Turillazzi, Aina, Mariarosaria Taddeo, Luciano Floridi, and Federico Casolari. 2023. The Digital Services Act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology* 15: 83–106. [CrossRef]

UNICEF. 2008. Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents. World Congress III Against Sexual Exploitation of Children and Adolescents. Available online: https://www.unicef.org/documents/world-congress-iii-against-sexual-exploitation-children-and-adolescents (accessed on 15 July 2024).

UNICEF. n.d. How We Protect Children's Rights with the UN Convention on the Rights of the Child. Available online: https://www.unicef.org.uk/what-we-do/un-convention-child-rights/ (accessed on 15 July 2024).

United Nations. 1990. Convention on the Rights of the Child. UN General Assembly Resolution 44/25. Available online: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (accessed on 15 July 2024).

United Nations. 2019. CRC/C/156: Guidelines Regarding the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. Available online: https://www.ohchr.org/en/documents/legal-standards-and-guidelines/crcc156-guidelines-regarding-implementation-optional (accessed on 18 July 2024).

UNODC. n.d. United Nations Office on Drugs and Crime Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Available online: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed on 18 July 2024).

van Daalen, Ot. 2023. The right to encryption: Privacy as preventing unlawful access. *Computer Law and Security Review* 49: 105804. [CrossRef]

van den Brink, Ton, Michael Hübner, Alexander Hoppe, Anna Citterbergová, Elaine Mak, and Anna Taimr. 2022. Flexible Implementation and the EU Sexual Abuse Directive. Available online: https://dspace.library.uu.nl/bitstream/handle/1874/421636/RSC_WP_2022_35.pdf?sequence=1 (accessed on 15 July 2024).

van Es, Laure. 2016. Virtual child pornography as potential remedy against child sexual abuse. *Biomedical and Health Sciences Research* 6: 166–73. [CrossRef]

WeProtect Global Alliance. 2023. Alarming Escalation in Child Sexual Abuse Online Revealed by Global Threat Assessment 2023. Available online: https://www.weprotect.org/wp-content/uploads/Global-Threat-Asssesment-2023-Press-Release.pdf (accessed on 11 July 2024).

Westlake, Bryce Garreth. 2020. The past, present, and future of online child sexual exploitation: Summarizing the evolution of production, distribution, and detection. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Edited by Thomas J. Holt and Adam M. Bossler. Cham: Palgrave Macmillan, pp. 1225–53.

Wilman, Folkert. 2022. The Digital Services Act (DSA)—An Overview. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4304586 (accessed on 18 July 2024).

Witting, Sabine K. 2021. Transnational by Default: Online Child Sexual Abuse Respects No Borders. *International Journal of Children's Rights* 29: 731–64. [CrossRef]

Witting, Sabine, and Mark Leiser. 2022. Expert Workshop on EU Proposed Regulation on Preventing and Combating Child Sexual Abuse. Available online: https://rm.coe.int/outcome-report-of-the-expert-workshop-on-eu-proposed-regulation-on-pre/1680aa00e4 (accessed on 21 June 2024).

World Economic Forum. 2022. Online Dangers for Children are Rife. We Must Both Pre-Empt Them and Treat the Consequences. Available online: https://www.weforum.org/agenda/2022/06/child-safety-protection-internet/ (accessed on 14 August 2024).

Zharova, Anna K. 2023. Internet service providers as subjects of prevention of sexual crime on the Internet. *Law Enforcement Review* 7: 72–82. [CrossRef]