Global Campus Europe

NOVA SCHOOL OF LAW

European Master's Programme in Human Rights and Democratisation

A.Y. 2024/2025

SYMBOLIC HARM AND DIGITAL ABUSE:
Towards a New Legal Framework for AI-Generated CSAM

Author: İrem Yener

Supervisor: Prof. Vera Lúcia Raposo

Word Count Declaration: 23.205

Abstract

The rapid development of artificial intelligence (AI) has presented significant ethical and legal challenges, particularly in the field of child's rights protection. This thesis asks: To what extent can AI-generated child sexual abuse material be criminalised under current national and international legal frameworks, particularly in the absence of real children as identifiable victims? While some AI-generated content may include a depiction of a real child's face, others are entirely synthetic creations that do not involve identifiable minors. This raises urgent questions regarding the definition of crime, harm, and victimhood within criminal law. This research focuses on examining to what extent such material can be prosecuted under existing legal frameworks and what legal interest is protected. Although no physical abuse occurs during the production of such content, unauthorized use of children's likenesses -whether real, altered or digital synthesized- raises serious legal and ethical concerns. The thesis also describes the current state of international and national legal regulation and argues that a differentiated legally sound approach to AI generated CSAM is urgently needed. Considering the potential for the normalisation of child abuse, identity harm and structural exploitation, this research argues for stronger normative responses that prioritize the best interest of the children in the digital age.

Keywords: artificial intelligence, child sexual abuse materials, deepfakes, AI-generated images, legal theories, criminal law.

Acknowledgements

Writing this thesis has been one of the most challenging intellectual and emotional journeys of my life. I am deeply grateful to everyone who accompanied me through this process -whether by offering guidance, standing by me in moments of crisis, or simply believing that I could finish what I started.

First and foremost, I would like to thank my thesis supervisor, Professor Vera Lucia Raposo, for her guidance throughout this process, and Professor Teresa Pizarro Beleza, my EMA Director, for her support. I owe special thanks to Professor Maria Beatriz Seabra Brito, who -although not formally my supervisor- offered me generous academic support and intellectual encouragement when I needed it most.

I would also like to thank to my teachers Judit Villena Rod and Orla Ní Cheallacháin from the Global Campus of Human Rights, whose presence, kindness, and unwavering support reminded me that there is space for vulnerability and compassion in academia. Knowing that they were there, gave me the courage to keep writing.

This thesis would not have been possible without the emotional support of my friends, especially Charlotte and Elif. In a year marked by uncertainty, burnout, and moments of deep solitude, they reminded me of who I am and why I started this journey in the first place. They listened to me complain, helped me process my anger and fear, and celebrated my smallest victories as if they were their own. In a year when I often felt like giving up, I found the strength to return and continue in them.

My deepest gratitude goes to my former organisation, the Association for Struggle Against Sexual Violence (Cinsel Şiddetle Mücadele Derneği). Working with survivors of sexual violence changed my life. It taught me to listen, to witness, and to carry the weight of stories that are not mine but that still demand responsibility. This thesis is, in many ways, a continuation of that journey. I owe everything to the women who trusted me with their stories, who fought for dignity and justice in a system that rarely offers either. What began as a path for women has led me to fight for children. I hope this work honours that legacy.

And finally, to the girls -real and imagined- who appear in pixels, in prompts, in courts, and in silence: I have written this for you. You are not invisible. You are not voiceless. And you are not forgotten. I will always remember you.

TABLE OF CONTENTS

CHAPTER I: INTRODUCTION

1. Background

This chapter outlines the key concepts that form the foundation of the thesis. At the same time, it functions as a literature review, offering a comprehensive conceptual framework on sexual violence and its manifestations in the cyber space.

1.1. AI-generated Images

The use of AI has transformed the way that industries operate, thus revolutionizing industries such as gaming, fashion, art, and even medicine. One area where this technology has had a significant impact is image generation. Thanks to techniques such as deep learning, generative adversarial networks (GANs), and diffusion models, AI systems can now produce highly realistic images oftentimes indistinguishable from real photographs.

These synthetic images can depict entirely fictional people, copy the likeness of real individuals without consent, or combine elements of real and fictional imagery through complex manipulations -often blurring the boundaries between these categories. Importantly, data plays a crucial role in modern machine learning (ML) systems. Datasets are the essence of computer vision tasks[1] and all types of AI. However, AI tools do not simply replicate their training data, but their outputs are fundamentally shaped and constrained by.

Realistic synthetic picture production tools are commonly utilized for artistic or business goals, but they also cause a lot of legal problems. Some pictures made by AI are completely fake, while others are based on genuine pictures in some way. Most of the time, the pictures of real people that are made from data are obtained without their wisdom or approval. The law is having a hard time keeping up with the lines between actual and fake material as they get more and more hazy. This is especially true when it comes to confidentiality, approval, slander, and criminal responsibility. That is to say, legal systems need to deal with a complicated mix of harm, responsibility, and legislation in the age of AI-generated pictures, but they have trouble keeping up with the pace of scientific change.

1 Yang, Z., et al (2023b, October 3). “AI-Generated Images as Data Source: The Dawn of Synthetic Era.” https://arxiv.org/abs/2310.01830

It is also important to make clear the difference between AI-generated photos and the greater well-known phrase "deepfakes." Deepfake is a combination of the words "deep learning" and "fake."[2] It describes photos or videos made with machine-learning methods that mix living photos and footage into origin along with movies. With a deepfake, anyone may switch out a person's face for another person's body in pictures or movies. Deepfakes may also change the original voice and facial expressions, making footage that looks and sounds very natural but is fake.[3] Deepfakes employ AI and deep learning to change the original face, voice, or emotions. Deepfakes are a type of AI-generated material. However, not all AI-generated photos are deepfakes.

Because deepfakes often involve the manipulation of real individuals' likenesses, lawmakers have been more proactive in regulating them. However, AI-generated images that do not involve identifiable real persons have received comparatively less legal attention, despite potentially posing similar risks in terms of harm and misuse.

1.2. Image-Based Sexual Abuse

Image-based sexual abuse refers to creating, distributing and/or threatening to distribute nude or sexually explicit images of individuals without their consent.[4] Those who commit these acts can be intimate partners, ex-partners, family members, friends, colleagues, or strangers. Even though image-based abuse can also be called 'revenge pornography' in some literature, revenge is not the sole purpose of image-based abuse. Partaking in this type of abuse is mainly fuelled by malicious intentions whether that be to profit, humiliate, harass, or control another person.

Image-based sexual abuse can occur in numerous ways, someone sharing (or threatening to share) intimate photos or videos of a person without their consent so that others, including the person's friends and family, can see them. The dissemination of the explicit material that forms content for image-based abuse usually takes one of two forms: offline, where the material is

[2] Hayley Tsukayama India McKinney Jamie Williams, "Congress Should Not Rush to Regulate Deepfakes" (*Electronic Frontier Foundation*, June 26, 2019) https://www.eff.org/deeplinks/2019/06/congress-should-not-rush-regulate-deepfakes

[3] Chadha, A., et al (2021). Deepfake: An Overview. In Lecture notes in networks and systems (pp. 557–566). https://doi.org/10.1007/978-981-16-0733-2_39

[4] Clare McGlynn and others, "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse" (2020) 30 Social & Legal Studies 541 https://doi.org/10.1177/0964663920947791

physically shown to other people through interactions with a live audience; or online, through various means such as uploads to email, social media, or pornographic sites.[5]

Image-based sexual abuse is a broad and complex term referred to various types of abusive behaviours that involve 'nude' or sexual images. The images can be created by the victim or can be produced consensually in an intimate relationship context. Alternatively, images may have been altered, created coercively, taken surreptitiously, during a sexual assault or rape.[6]

In the last few years, a new version of image-based sexual abuse has been circulating online; AI-generated sexually abuse materials. The advancement of artificial intelligence catapulted the release of tools and websites that nudify images or turn images into pornographic content. There are excessively websites, such as Nudify.me or Clothoff, which are still open and accessible for everyone, without requiring any technical skills. Clothoff requires membership with money or coins, but common people's pictures can be uploaded. Conversely, Nudify.me allows access to a large number of pictures or videos, content mostly belonging to well-known women, without any membership. The website also contains guides for nude image creation in their blog section.[7]

While many of these tools are used to target adult women in public, such technologies have also been known to be used to produce AI-based child sexual abuse material, which depicts children in sexualized ways, even if it does not involve actual abuse.

1.3. Child Sexual Abuse Materials

Child Sexual Abuse Material (CSAM) refers to as imagery or videos which show a person who is a child and engaged in or is depicted as being engaged in explicit sexual activity.[8] It shows photos, videos, or digitally created content depicting minors in sexualized contexts. Unlike the term "child pornography," the term CSAM emphasizes the abusive and criminal nature of the material. Due to, in 2016, an international working group, comprising a collection of countries

---

[5] Chidera Okolie, "Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns" (*Virtual Commons - Bridgewater State University*) https://vc.bridgew.edu/jiws/vol25/iss2/11/?utm_source=vc.bridgew.edu%2Fjiws%2Fvol25%2Fiss2%2F11&utm_medium=PDF&utm_campaign=PDFCoverPages

[6] Nicola Henry, Asher Flynn and Anastasia Powell "Image-Based Sexual Abuse: Victims and Perpetrators," vol No. 572 (Australian Institute of Criminology, 2019) https://www.aic.gov.au/sites/default/files/2020-05/imagebased_sexual_abuse_victims_and_perpetrators.pdf

[7] *'A Step-by-Step Guide to Nudifying Photos'* (Nudify Blog) https://www.nudify.me/blog/a-step-by-step-guide-to-nudifying-photos accessed 30 June 2025.

[8] "What Is Child Sexual Abuse Material?" https://www.inhope.org/EN/articles/child-sexual-abuse-material

and international organizations working to combat child exploitation, formally recognized "child sexual abuse material" as the preferred term.[9]

Child sexual abuse material (CSAM) is not only a violation of a child's bodily autonomy, but it is also a record of crime that is shared and consumed for pleasure. These things are proof of trauma that lasts long after the abuse has happened. Survivors' stories make it clear that victims often feel like they are "eternally abused" because their images are still out there online, which makes it very hard to heal.[10]

Even though people are more aware of and enforce the law, access to CSAM has grown around the world as technology has improved. In a big operation in early 1990s, police might have taken a few thousand pictures, but one person can have hundreds of thousands of files these days.[11] This rise is directly related to internet's role in allowing instant, anonymous sharing and encrypted forums that make it normal and easy to trade abusive materials.[12]

In the past, making this kind of content illegal has mostly been about content that shows real minors. Yet, a legal and ethical dilemma arises with the emergence of hyper-realistic, AI-generated images that depict fictional minors in sexualized ways. While no physical child may be involved in the creation of such images, their content arguably mimics and normalises the abuse of real children. Scholar like Al-Alosi question whether legal systems should tolerate such "fantasy material" under the guise of freedom of expression, especially when the depicted harm is suggestive of real exploitation.[13]

In this context, worldwide agreements like the Alternative the Covenant for UN The Agreement upon the Rights of the Child currently include a large definition of child pornography. It includes any portrayal "by whatever means" of adolescents participated in sexual activities,

[9] US Department of Justice and National Center for Missing & Exploited Children (NCMEC), Child Sexual Abuse Material: Federal Response and Strategic Recommendations (2023) https://www.missingkids.org/content/ncmec/en/ourwork/impact.html#reduceexploitation accessed 30 June 2025.
[10] Ring S, Gleeson K and Stevenson K, *Child Sexual Abuse Reported by Adult Survivors* (Routledge 2022) https://www.routledge.com/Routledge-SOLON-Explorations-in-Crime-and-Criminal-Justice-Histories/book-series/HCCJ
[11] Hadeel Al-Alosi, *The Criminalisation of Fantasy Material: Law and Sexually Explicit Representations of Fictional Children* (Routledge 2018) https://lccn.loc.gov/2018001996 23-26.
[12] Ibid 40-44.
[13] Al-Alosi (n 11) ch 1.

which might include computer-generated images[14]. Also, child safety organizations have shown that many violators whose watch AI-generated or altered content go upon committing interaction offenses, which goes against the idea that this kind of substance is a safe way to get rid of stress.[15]

Finally, the rise about instruments and online pages like Nudify.me, which let anybody make naked or sexualized pictures of celebrities or youngsters using AI without needing to know how to code, shows a serious lack of regulation. These kinds of technologies not only make it easier for people to spy on and harass others, but they have also been used to make fake child abuse content[16]. The line between genuine and fake grows less obvious legally and ethically, but the risk of damage is still very evident and urgent.

1.4. AI-Generated Child Sexual Abuse Materials

Virtual CSAM is a new and very worrying type of child sexual abuse material that has come about because of advances in technology. This word describes sexually explicit images of youngsters made without utilizing any real children, using computerized tools like AI.[17] Fully AI-generated CSAM is one of the most important types of CSAM. These pictures of made-up kids in sexual situations are made solely by machine learning models, usually generative adversarial networks (GANs). There are no real-life sources for these pictures.[18]

AI-generated CSAM and AI-manipulated CSAM are the two primary forms of virtual CSAM. AI-generated CSAM is made up of pictures or videos of kids who don't exist. AI-manipulated CSAM, on the other hand, changes pictures or videos of real kids to show them in sexual situations.[19] These two main forms can be broken down into smaller groups, such as photorealistic, morphed, and abuse-trained CSAM.[20]

---

[14] United Nations, "Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography," vols 2171–2171 (2000) https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/crc-sale.pdf

[15] Juliane A Kloess and others, "The Challenges of Identifying and Classifying Child Sexual Abuse Material" (2017) 31 Sexual Abuse 173 https://doi.org/10.1177/1079063217724768

[16] Nudify Blog (n 7).

[17] Shruthi Krishna, Fiona Dubrosa and Ruth Milanaik, "Rising Threats of AI-Driven Child Sexual Abuse Material" (2024) 153 PEDIATRICS https://doi.org/10.1542/peds.2023-063954

[18] Maria Lazaridou, "Schrödinger's Crime: AI-Generated Child Sexual Abuse Material as a Victimless Offense" (2024)

[19] Krishna S et al (n 17), 2-3

[20] Cezarita Cordeiro V, "Combating the Rise of AI-Generated Child Sexual Abuse Material" (2025) https://www.humanium.org/en/combating-the-rise-of-ai-generated-child-sexual-abuse-material/

Photorealistic CSAM is a term for photos which have been completely fake yet look almost exactly like pictures of actual kids. They typically employ precise suggestions or simulation learning for copy illumination, anatomy, and stance alongside scary accuracy. Transformed CSAM mixes actual children's faces with bodies or circumstances for render that look like sexual actions are happening. This makes it somewhat grounded and hence more legally complicated.[21] Abuse-trained CSAM is a term for pictures produced through algorithms which were intentionally developed on real CSAM datasets. The training process includes illegal material, which raises distinct moral and legal issues, even nevertheless the product is fake.[22]

AI-generated CSAM pushes the limits of current constitutional terms as well as ethical instincts, whereas conventional CSAM includes actual children and is therefore directly harmful and abusive. There isn't an obvious victim, and it was made without a crime happening in the real world. But the realistic quality and aim beneath this kind of video make it hard to tell the difference among "fantasy" and exploitation substance. This might make child sexual abuse seem usual or increase desire for genuine CSAM.[23]

1.5. Legal Concerns About AI-Generated CSAM

The rise of AI-generated CSAM makes it very unclear how present laws will be used and what they will cover. The majority laws make it illegal to make and own CSAM that involves actual kids, but they don't always have obvious rules against imitation material. Lazaridou[24] says that the judicial system has a hard time dealing with things that look like abuse but don't have the casualty. This lack of clarity is especially bad in places where laws against child pornography are closely tied to the existence of a genuine, recognized kid and bodily damage.

AI-generated CSAM might also make it harder to safeguard children by making it harder to indicate and making it harder to figure out what to investigate first. The Internet Watch Foundation (IWF) discovered that greater compared to 20,000 AI-generated photos were submitted to a single dark web forum in only one month. Further than fifty percent of these

[21] Amy Trivison "Understanding the Line between Art and Abuse: How Generative AI Changes the Landscape of Child Sexual Abuse Materials," vol 33 (2024) journal-article https://scholarship.law.edu/jlt/vol33/iss1/6
[22] Lazaridou M (n 18), 40.
[23] Trivison (n 21), 90.
[24] Lazaridou M (n 18), 57.

photos were marked as being of criminal concern.[25] It is hard for police to tell when these pictures show genuine or made-up kids, which makes their jobs harder while might take consideration away to situations when someone is about to be hurt.[26]

While the relatively little legal debate regarding clearly synthetic, photorealistic AI-generated CSAM, subtypes such as morphed CSAM raise complex challenges within criminal law. These materials frequently involve the digital fusion of real children's facial features with adult bodies or sexual contexts. As such, they blur the distinction between fiction and exploitation, complicating the legal interpretation of fundamental terms like harm and victim. This hybrid nature introduces ambiguity that strains the doctrinal limits of child protection laws.[27] Given this complexity, and in line with the thesis's criminal law perspective, the following analysis will focus specifically on morphed CSAM -where the most pressing normative and conceptual debates are likely to unfold.

2. Research Questions and Objectives

This thesis intends to critically analyses the legal handling of AI-generated CSAM throughout the wider context of criminal law, concentrating on the issues provided by the lack of real-life victims. The main goal is to find out if traditional criminal law principles, especially people centred around damage and causality, employ that new type of abusive substance and what changes to the law or how it is understood may be needed to ensure what is done is operational and morally noise.

The main issue that this study tries to answer is, "How much can AI-generated CSAM be made illegal under current international laws, especially when there aren't any real children who can be identified as victims?" This primary issue illustrates increasing worries within constitutional research alongside usage: as AI technologies create hyper-realistic sexualized photos of kids, frequently lacking regarding all kids, they show that laws that were based on the existence of true individuals along with quantifiable damage are not always effective.[28]

---

[25] Trivison (n 21), 92.
[26] Internet Watch Foundation, "How AI Is Being Abused to Create Child Sexual Abuse Imagery" (2023) report https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf
[27] Witting SK, "Child Sexual Abuse in the Digital Era: Rethinking Legal Frameworks and Transnational Law Enforcement Collaboration" (2020) https://hdl.handle.net/1887/96242
[28] Katalin Parti and Judit Szabó, *'The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe'* (2024) 13 *Laws* 67 https://doi.org/10.3390/laws13060067

The thesis goes into more detail on a few goals that are all connected. Initially, this looks at how AI-generated CSAM, especially photos of actual children's faces that have been altered, contradicts the usual concepts of injury, victim, and malicious intention. That mixed photographs are in a legal grey area, which makes people rethink established ideas about criminal law. Secondly, it looks at whether culpability can be based on preventing damage instead of its appearance, implementing through consideration passive social and emotional effects like the normalizing of neglect, desensitizing, or the possibility of escalating interactions with offenses.

Third, the thesis looks at whether the current legal categories for morphing CSAM, such as manufacturing, ownership, and propagation, are good enough to capture the distinctive ways that AI-generated material is made and shared. Finally, it looks at whether the current legal systems, such as those in the EU, the US, and worldwide legislation, offer enough safeguarding, and there are still deficiencies that need to be filled by standard explanation and constitutional change.

This thesis looks at morphing CSAM from a legal point of view. The goal of the study is to help with changes to criminal law that safeguard children's rights while still following the basic rules of legitimacy alongside the ratio.[29]

3. State of Art

The criminal responsibility of AI-generated child sexual abuse material (CSAM) has become a complicated problem that touches on law, ethics, and technology that is changing quickly. The main issue in this argument is the unsolved conflict between the absence of direct harm to actual children in making synthetic material and the bigger threats to society that come from its spread. To make things further clearer, the rise of synthetic or AI-generated images has thrown off the traditional constitutional groups where CSAM has been researched in relation to real children. Most laws throughout the world haven't been changed yet to make it clear that

[29] Insoll T and others, "Risk Factors for Child Sexual Abuse Material Users Contacting Children Online" (2022) Journal of Online Trust and Safety https://doi.org/10.54501/jots.v1i2.29

AI-generated CSAM is illegal.[30] This means that AI-generated photos are still in a gray area. So, there is still a lot of operation to be done to clear up the confusion about the rules related to these substances, especially in European countries, fill in the gaps in execution plans, and provide obvious constitutional structures.

The Supreme Court of the United States ruled in New York v. Ferber (1982) that child pornography is not protected speech. This means that the government can make it illegal to make or own it in order to protect the health and safety of children.[31] The Court, on the other hand, said in Ashcroft v. Free Speech Coalition (2002) that virtual CSAM is different from pictures of actual children since there are no real victims in the virtual world.[32] But as generative AI becomes better, this split is becoming harder to defend. Hyper-realistic fake CSAM makes it hard for law enforcement to tell the difference between fake and real images, which makes it hard to gather evidence and enforce the law.[33]

The effects of CSAM on victims are well-documented and deeply harmful, including long-term psychological trauma, difficulties in relationship, and the continued circulation of abuse material online.[34] Even in the absence of real victims, synthetic material has been found to perpetuate indirect harms. These include normalization of paedophilic behaviour, use as a grooming tool, and reliance on training datasets that often include real CSAM, thus re-traumatizing survivors.[35]

Conversely, critics argue that overly broad criminalization risks infringing on constitutional freedoms of stifling digital creativity. This tension has led to diverse legislative responses. In the U.S., states such as California and Virginia have enacted laws criminalizing AI-generated CSAM that is "virtually indistinguishable" from real imagery, while federal responses remain cautious due to First Amendment protections.[36]

---

[30] Emmanouela Kokolaki , Paraskevi Fragopoulou, "Unveiling AI's Threats to Child Protection: Regulatory efforts to Criminalize AI Generated CSAM and Emerging Children's Rights Violation". *Institute of Computer Science.* (2024). SafeLine, 1. https://arxiv.org/pdf/2503.00433

[31] *New York v. Ferber*, 458 US 747 (1982) https://supreme.justia.com/cases/federal/us/458/747/.

[32] *Ashcroft v. Free Speech Coalition*, 535 US 234 (2002) https://supreme.justia.com/cases/federal/us/535/234/.

[33] Ibid.

[34] Cynthia DeLago and others, "Children Who Engaged in Interpersonal Problematic Sexual Behaviors" (2019) 105 Child Abuse & Neglect 104260 https://doi.org/10.1016/j.chiabu.2019.104260

[35] "Bill Text - AB-1831 Crimes: Child Pornography." https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1831

[36] AB-1831 (n 35); Virginia Code § 18.2-374.1.

The initial idea for the Child Sexual Abuse Regulation in Europe was to make "realistic synthetic depictions" illegal in a way that didn't favour any one type of ad technology.[37] The European Parliament passed a new version of the Regulation in June 2024, however it is very different from prior proposals.[38] It now clearly says that Member States must make it illegal to not just have and share AI-generated CSAM that genuinely shows a kid, but also to make it, even if there isn't an actual child there. The statement makes it clear that this kind of fake material is subject to the same criminal laws as actual child material. This shows a firmer stance against fake child sexual abuse materials. This new version is more in line with the UK's long-standing ban on "pseudo-photographs," which makes AI-generated CSAM a crime under the Protection of Children Act 1978[39] and the Coroners and Justice Act 2009.[40]

Further big problem is figuring out who is responsible over AI-generated material that is illegal. Because such structures don't have purpose and acquire on their own, constitutional experts disagree on who ought to be responsible: creators, structure suppliers, or consumers. AI instruments may be used for either good and bad objectives, that makes things even more confusing. Politicians need to find the right equilibrium between protecting children and letting people speak their minds and letting technology grow. Regulation problems get worse when productive instruments are available all over the world, because criminals can take advantage of variances in laws across countries. Supporters for victims' rights say that allowing synthetic CSAM to spread freely makes abuse worse and destroys societal standards which protect minors.

Even if there is no physical injury, current laws are still very much linked to the need for a real kid or actual harm. But the increasing social, mental, and physical damages associated with synthetic CSAM show that we require fresh legislation. New laws are starting to use criteria like reality and social danger more and more. They see suffering not merely as a crime against one person, however as a danger for kids' security and public order as a whole. The following change is part of a larger trend toward recognizing which damage in the online ages frequently goes beyond bodily limits and needs rules which can deal with either direct and indirect abuse.

[37] Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography [2011] OJ L335 https://eur-lex.europa.eu/eli/dir/2011/93/oj/eng
[38] "Fight against Child Sexual Abuse: Updated Rules to Address New Technologies | News | European Parliament" https://www.europarl.europa.eu/news/en/press-room/20250613IPR28905/fight-against-child-sexual-abuse-updated-rules-to-address-new-technologies
[39] Protection of Children Act 1978 (UK) https://www.legislation.gov.uk/ukpga/1978/37
[40] Coroners and Justice Act 2009 (UK) https://www.legislation.gov.uk/ukpga/2009/25/contents

4. Methodology

This thesis adopts a qualitative legal research methodology, combining doctrinal analysis with comparative legal reasoning to examine how national and international legal frameworks respond to the emerging challenges posed by AI-generated child sexual abuse material. The doctrinal method enables a critical interpretation of primary legal texts, such as EU directives, national criminal statues, and international conventions in order to clarify the normative structure, legal logic, and scope of current criminalisation approaches. This method was chosen due to the primarily normative and conceptual nature of the research question, which interrogates the legal status of AI-CSAMs but raises significant questions about symbolic and structural harm.

In addition to primary sources, the thesis engages with a broad range of secondary literature, including doctrinal commentaries, legal journals, AI ethics scholarship, and institutional reports from NGOs (e.g., Internet Watch Foundation, ECPAT), academic working groups, and transnational policy bodies. These sources were analysed thematically to identify recurring legal, moral, and regulatory concerns related to AI-CSAM, with particular focus on the evolving definitions of harm, intent, and victimhood.

A comparative legal approach is employed to identify the normative divergences and overlaps in how different jurisdictions conceptualise and regulate AI-generated CSAM. This method focuses different countries' legal frameworks, selected due to their fundamentally different legal systems, which significantly influence not only the content of criminal law but also the principles underpinning its interpretation and enforcement. These jurisdictions offer distinct perspectives on crime definition, criminalisation thresholds, and prosecutorial discretion, making them particularly valuable for analysing how emerging harms like AI-generated CSAM are addressed in practice.

Specifically, the thesis contrasts harm-based models of criminalisation in Europe or intent-based approaches found in parts of the US. It critically evaluates key criminal law doctrines - such as *mens rea*- to assess their adequacy in responding to synthetic sexual offences. Relevant legal instruments analysed include the EU AI Act, GDPR, UK's Criminal Justice and Public Order Act (1994), and California’s Assembly Bill 1831, among others. Through this

comparison, the research aims to highlight the legal, philosophical, and procedural differences in criminalising AI-CSAM across different legal traditions.

The data analysed in this thesis primarily consists of legislative texts, case law, policy reports, and academic commentary relevant to the regulation of artificial intelligence and child sexual abuse material. These materials are subjected to doctrinal and interpretive analysis, involving close reading, thematic categorisation, and critical comparison across jurisdictions. The focus is on how different legal systems define and use important criminal law ideas when it comes to non-physical and synthetic crimes.

Nonetheless, the chosen methodology has certain limitations. Firstly, the legal landscape concerning AI-generated CSAM is rapidly evolving, and during the writing process, several significant legislative developments occurred -for instance Eu Directive 2011/93/EU. These developments have required an adaptive approach to the research question, shifting the thesis' focus from "identifying legal gaps" to "evaluating how current frameworks address normative and doctrinal challenges". Finally, the absence of harmonised global standards limits the generalisability of some findings.

5. Conclusion

The emergence of AI-generated child sexual abuse material (AI-CSAM) challenges long-standing assumptions in law about what constitutes abuse, harm, and criminality. This chapter has outlined how generative technologies -while capable of immense societal benefit- have simultaneously introduced new forms of exploitation that evade conventional definitions. Unlike traditional CSAM, synthetic content complicates legal responsibility by removing the direct presence of a physical victim, yet its production and circulation continue to contribute to the normalization of child sexualization and psychological harm. The current regulatory vacuum surrounding AI-generated imagery, particularly morphed and photorealistic forms, reveals a deep disjunction between technological advancement and legal evolution.

Furthermore, the chapter has situated AI-CSAM within the broader context of image-based sexual abuse, child protection frameworks, criminal law and international law. It has introduced the legal, ethical, and conceptual dilemmas posed by fictional representations that mimic real abuse, while establishing morphed CSAM as the focal point of analysis. As the next chapter

will explore, criminal law must grapple with how to conceptualize crime and victimhood in a landscape where harm is structural, symbolic, and anticipatory. The need for a doctrinal and normative reconfiguration is pressing, as current frameworks fail to capture the unique risks posed by AI-generated depictions of child abuse.

CHAPTER II: LEGAL THEORIES

1. Criminal Law Theories

George P. Fletcher once questioned, "Where does legislation start?" and responded, "Law starts in disputes." Laws that control how people act might not be necessary if there were no disputes.[41] This remark additionally puts law in the context of social conflicts, however that additionally gives us a basic way for think how legal systems have changed throughout time, specifically criminal law. Ethics, politics views, and possible considerations about why the community ought to handle deal with misconduct had what had an effect on criminal law ideas across moment.

People usually think of criminal law as a set of rules that stop people from doing things that are hurtful, terrifying, or illicit in nature, mostly by punishing them. Fletcher's idea which "law starts alongside dispute" shows how criminal law may help settle those disputes by using ideas like damage, shame, alongside constitutional accountability. But those basic ideas were not set in stone; they possess changed throughout time via complicated logical arguments, especially over the intent or legitimacy for retribution.

Retaliation, pragmatics, and rejuvenating justice are examples of ideas of punishment that have traditionally affected both the moral and practical reasons for punishing criminals. Retributive methods focus on the offender's moral desert and the need to fix the moral imbalance that the crime generated.[42] Utilitarian ideas, on the other hand, put societal benefit first and try to stop future crimes by either deterring them or helping the people who commit them.[43] Restorative justice, on the other hand, tries to fix the damage performed for both parties by promoting conversation, responsibility, and making things right instead of punishment.[44]

Those structures had worked well to deal with common types about damage, like bodily assault, property crimes, or additionally emotional assault, when the victims and the effects are clear and can be tracked. But the increase of cybercrimes presents serious philosophical and moral problems. These crimes may not have a kid who was hurt and a clear cause, but they

[41] George Philip Fletcher, *The Grammar of Criminal Law: American, Comparative, and International Volume One: Foundations* (Oxford University Press 2007).
[42] Jean Hampton, 'The Moral Education Theory of Punishment' (1984) 13 *Philosophy & Public Affairs,* 208.
[43] Joel Feinberg, 'The Expressive Function of Punishment' (1965).
[44] Howard Zehr and Ali Gohar, *The Little Book of Restorative Justice* (Good Books 2003), 2-4.

nonetheless seem to deserve resilient ethical rebuke and constitutional action. The lack of a clearly identified victim makes it harder to use standard permitted ideas such as mens rea, guilt, and injury.[45]

Also, when AI systems add new levels of independence, lack of transparency, and shared responsibility, existing frameworks have a hard time answering the most important question: Who is the offender? Where is the damage? What are we penalizing? In response, legal academics have started to urge for a re-evolution of the basic ideas behind criminal law to include these damages that aren't based on people, where neither the perpetrator nor the victim fits with traditional ideas of culpability and suffering.[46]

In light of this, this section wants to look at how useful and limited conventional retribution concepts include, especially when they are used to deal with new online damages. AI-generated sexual abuse material is forcing the legal system to deal with the collapse of basic classifications like crime, harm, and victim. This means that it is not only required to reconsider the philosophical basis of criminal law, yet also critical.

a. Nature of Punishment

Retribution on criminal law isn't only about following the rules; it's also a moral and intellectual issue which shows what a community believes is right and wrong. Any logical explanation of criminal responsibility must start by asking? What does punishment mean? Why is it okay? When is it okay to impose it? Positive law can tell us when and how to punish someone, but it is its theoretical basis which provide us a way to grasp their significance and credibility. Joel Feinberg infamously said that punishment is not just a way to stop others from doing something wrong or get back at them; it is also a way to "express" yourself. Feinberg says that punishment is a way for society to show that it disapproves of a bad behaviour. It is a normal way for people to show their anger, resentment, and disapproval.[47] This approach says that punishment does more than just chastise; it additionally reinforces the rule of law and confirms ethical limitations that everyone agrees on. The expressing behave is what makes lawful retribution different of just punishments, that might hurt people yet don't have any ethical meaning.[48]

[45] Alan Brudner, *Punishment and Freedom* (Oxford University Press 2009), 179.
[46] Douglas Husak, *Overcriminalization: The Limits of the Criminal Law* (Oxford University Press 2008), 104.
[47] Feinberg (n 43) 400.
[48] Ibid, 401.

Feinberg goes into more detail about this point of judge through separating retribution into two main parts: harsh attitudes and condemning symbols. He stresses that retribution is valid because it has two sides: the bodily starvation it causes and the ethical condemnation it sends. This is particularly clear in situations where the level of punishment is adjusted to show different levels of societal disapproval.[49]

This expressive way of thinking about retribution possesses grow quite important in current criminal law. In his important book on the language of criminal law, George Fletcher says that retribution must be seen with a fundamental lens. Each court has to address all three important questions: What is wrong? Who is a culpable agent? And what does punishment do for society or morals?[50] Those concerns rather just affect why we define crime, yet they also affect the way we justify retribution ethically.

Mitchell Berman added to this conversation through pointing out the two sides of retribution: its revengeful basis and its usefulness. Retaliation says that punishment is fair because of ethical deserts whereas deterministic views say that retribution is fair because of its consequences, like discouragement, standard encouragement, or incapacity. Berman, on the other hand, doubts whether both methods adequately convey why complicated punishment is in current law. He says that any meaningful rationale must include both figurative and expressing aspects.[51]

Feinberg also lists several derived figurative purposes which retribution serves, such as imposing rejection, figurative non-acquiescence, and accessible validation. This performs assist clarify how some actions has to be criticized additionally as they don't do much destruction, including when they go against group ideals or are symbolic offenses.[52] This is still important today, as seen in the argument across AI-generated child sexual misconduct content, in which criticism might not be aimed at a specific victim but at reinforcing acceptable behaviours online. In the end, retribution is what it is because it can show what people principles, stop people from breaking the law again, and keep society's morals strong. Because of this, it's not enough to think of punishment as only a way to respond to injury. That has to additionally become a way for the legal system to express and uphold its many basic promises.

[49] Ibid, 403
[50] Fletcher (n 41) 59.
[51] Mitchell N Berman and The University of Chicago, “Punishment and Justification” (2008) 118 Ethics, 258.
[52] Feinberg (n 43), 405.

b. The Philosophical of Punishment

In philosophy, the notion of punishment has a long and complicated history. At its heart is the question: Why should we punish anyone? Over the years, legal experts and moral philosophers have given diverse solutions based on their own ideas of justice, damage, and social order. There are a lot of different views, but three main ones stand out: retributivism, utilitarianism, and restorative justice. Each one has a different reason for punishing someone, such as moral desert, social usefulness, or community restoration.

Retributivism says that punishment is a moral way to deal with wrongdoings. This view says that punishment is right because the person who did wrong deserves it, not because of what may happen in the future. Michael Moore famously said this when he said, "punishment is justified by the moral culpability of those who receive it."[53] This point of view is based on proportionality: punishment should fit the crime, not go beyond it, and not be justified by any other benefit. Joel Feinberg also calls this framework one in which "moral guilt is both a necessary and sufficient condition for justified punishment."[54]

Herbert Morris provides an equitable aspect for that argument by saying that breaking the law is a violation of the interpersonal compact and that everyone will follow the law.[55] Morris says the retribution makes things reasonable again by taking away the "unfair advantage" that the criminal had. Jean Hampton, on the other hand, sees punishment as a way to send a moral message that the criminal's disregard for the victim is wrong and that the victim is just as morally valuable as the criminal.[56] However, these moral retributivist theories have trouble figuring out which moral wrongs should be punished by the law and how retribution must become proportional to ethical responsibility.

Legally vengeance moves the attention about ethical deserts for constitutional power in order to get rid of these kinds of uncertainties. For instance, Herbert Fingarette says that punishment is not a reaction with ethical inability in and of itself, but rather a necessary way for the law to show its normative power. He thinks that the law has to punish people who break it in order to

[53] Michael Moore, "The Moral Worth of Retribution," *Oxford University Press eBooks* (2010) https://doi.org/10.1093/acprof:oso/9780199599493.003.0003 179.
[54] Joel Feinberg, "The Classic Debate", in Philosophy of Law (Boston, MA: Cengage Learning, 2004), 627.
[55] Moore (n 53) 179.
[56] Hampton (n 42) 302.

keep its power; otherwise, its orders don't mean anything. So, punishment "humbles the will" of the person who did wrong and reestablishes the power of the law.[57] Alan Brudner also justifies punishment as a "self-willed" result of one's own legal decisions, based on a fictitious societal agreement which puts autonomy and authorized consistency first.[58]

Utilitarianism, by contrast, emphasizes outcomes. Under this theory, punishment is justified only if it produces net social benefits such as deterrence, rehabilitation, or incapacitation. Joel Feinberg describes utilitarian punishment as justified when it contributes to correction or prevention and recommends only that degree of punishment which produces "the most good or the least harm."[59] Berman supports a dual-structure theory that acknowledges retributive principles but argues for punishment's justification in its instrumental value as well.[60] Still, critics worry that strict utilitarianism risks sacrificing individual rights to achieve general utility, thereby legitimising excessive or even unjust punishment if it serves a broader social purpose.

Restorative justice puts the requirements for victims, criminals, and groups first, which goes against either paradigm. Restorative justice approaches don't concentrate upon accuse or punishment; instead, they try to fix the damage, encourage responsibility, and help people recover. Howard Zehr and John Braithwaite have both talked about this concept, which sees justice as a process that involves relationships and participation. It promotes controlled discourse, compensation, and shared acknowledgment, alongside the goal of restoring ethical equilibrium lacking using pain or being excluded.[61] People frequently don't regard it as a retribution alternative; instead, they see it as a way to fill in the blanks departed by revengeful and practical methods.

Rehabilitation law doesn't throw out punishment or effectiveness; instead, it makes them better with a more complete picture of damage and how to make it right. An authority said that "restoring fairness restores, enhances, and increases the basic ideas behind those retribution ideas" lacking completely rejecting for them.

---

[57] Herbert Fingarette, 'Punishment and Suffering' (1977) 50 *Proceedings and Addresses of the American Philosophical Association* 499.
[58] Brudner (n 45) 2.
[59] Feinberg (n 54) 627.
[60] Berman (n 51) 260.
[61] Howard Zehr, *Changing Lenses: A New Focus for Crime and Justice* (Herald Press 1995); John Braithwaite, *Restorative Justice and Responsive Regulation* (Oxford University Press 2001) 181.

These ideas offer different reasons over retribution that are ethical, permitted, along with feasible. Everyone has unique problems: vengeance might put pain above gain, selfishness might ignore equality in Favor of outcomes, and restorative justice might not become clear about how to punish. But to judge modern punishment techniques, you need to know how they work together. These conflicts get worse when new crimes happen, including those that happen with machine learning, where the damage is abstraction and the victim is not real. So, studying the logical basis of retribution helps us figure out if present laws can handle new kinds of crime, or if we need to come up with greater flexible systems.

2. The Challenge of Harm, Intent and Legal Interest on Sexual Offence

Recent technological developments have deeply disrupted long-standing assumptions in criminal law, particularly in the context of sexual offences. The emergence of AI-generated child sexual abuse material (AI-CSAM), especially in photorealistic or deepfake forms, has called into question the conceptual sufficiency of foundational legal elements such as harm, intent, and legal interest. Traditional criminal frameworks, shaped by the presence of a victim, a culpable actor, and an identifiable public or private interest to be protected, are being strained by crimes where no actual physical contact or direct human victim can be identified. Yet, these digital acts still provoke profound societal concern and raise demands for criminalisation. This section explores each of these three concepts -harm, intent, and legal interest- in both their doctrinal grounding and their challenged application in the AI-CSAM context.

In conventional criminal theory, "harm" is what makes it lawful to make anything a crime. Joel Feinberg is well-known for saying that "the harm rule" is the main constraint on how criminal law may be used.[62] This means that the government can only punish those who damage other people. This pain has to be genuine, definite, and quantifiable, such as a physical injury or obvious mental disability. Husak also says that criminal law ought to pertain to behaviours that cause unfair harm and that it shouldn't be expanded for involve things that are merely rude or wrong.[63]

But even in traditional ways of thinking, the notion of harm has transformed to mean more than

[62] Joel Feinberg, *Harm to Self: The Moral Limits of the Criminal Law* (Oxford University Press 1984) 26.
[63] Husak (n 46), 68.

just becoming hurt physically. Feinberg himself said that there are losses that are indirect or symbolic, such those that affect a person's ethical positioned image, or confidence in a group.[64] This trend is already obvious in sexual crimes, in which voyeurism and image-based abuse are both against the law. In many circumstances, the injury is not actual assault however a violation of confidentiality or respect.

AI-generated CSAM goes against this paradigm because it doesn't include an actual victim. But, as other academics have said, the suffering continues within inverse, cultural and figurative ways. Maria Lazaridou says that AI-CSAM might not portray an actual kid, but it nevertheless does "moral harm by demeaning the societal significance of youth and altering sexual standards."[65] This kind of stuff may keep paedophilic need alive, increase the need over genuine violence, and lead to "grooming through fantasy," which is a way to hurt others in the real world.[66] Research on how people use non-contract CSAM shows that people who use it typically go upon with commit interaction offenses, which supports the idea which this kind of substance is criminalizing.[67]

Additionally, survivors of youth sexually exploitation say that also AI-generated images may become retraumatizing when they include their name or appearance, because the picture represents a continual contravention of their identities and freedom.[68] The IWF's 2023 study similarly talks about the way AI techniques are utilized for "recreate" actual those targeted in made-up exploitation situations, mixing real and made-up damage in a worrying way.[69] These results show that the damage concept has to include not just physical pain yet figurative, interaction, and predicting damage.

People rea, or intention, usually means the guilty thought of the actor the intentional choice to do something wrong. Duff says that being responsible for a crime is linked to being able to answer for your acts, which means that you did them on purpose and willingly.[70] In sexual

[64] Feinberg (n 62), 400-403.
[65] Lazaridou (n 18) 47.
[66] Witting (n 27) 163.
[67] Kloess (n 15) 114.
[68] Salter M and Wong T, "Parental Production of Child Sexual Abuse Material: A Critical Review" (2023) 25 Trauma Violence & Abuse 1826 https://doi.org/10.1177/15248380231195891 18, 22.
[69] Internet Watch Foundation (IWF), *AI-Generated CSAM Report* (2023) https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf 6.
[70] Robin Antony Duff, "Answering For Crime" (2006) 106 Proceedings of the Aristotelian Society 87 https://doi.org/10.1111/j.1467-9264.2006.00140.x 123.

crimes, the purpose is looked at very seriously, especially when it comes to knowing that the victim didn't provide permission, their age, or the fact that the abuse was premeditated. This idea of guilt is what makes retribution morally right.[71]

When AI makes illegal stuff, it messes with this doctrinal clarity. Who has the intent: the user, the developer, or the AI itself? If someone inputs a text swift that makes something that looks like CSAM, are they guilty of trying to make that kind of content or just being careless? Lazaridou suggests a notion of "assigned purpose," who suggests the AI functions as an expansion of the user's determination. This means that the user is still responsible for the crime even if they didn't really make it.[72]

When AI changes or combines material on its own based on suggestions that appear harmless, figuring out what the AI meant to do gets harder. Some researchers say humans can fail to completely comprehend what productive examples produce, which makes it hard to predict what will happen and who is to blame. But if users knowingly change requests, particularly if they know how the system works, it shows which intention may become concluded when they act alongside understanding of possible criminal outcomes.[73]

Moreover, platform-level actors may also bear intent-like responsibility. As Salter and Wong argue, the production and circulation of AI-generated CSAM on platform that knowingly allow or ignore such content can be seen as “institutional failure of intent”, where failure to act constitutes complicity.[74]

Legal interest refers to the values and interests that criminal law exists to protect life, bodily integrity, property, public order. According to Fletcher, criminal law requires not just the violation of a rule but a wrong that offends a legitimate legal interest.[75] Feinberg similarly argued that criminalisation must rest on the protection of interests deemed valuable in a liberal

[71] Moore (n 53) 182.
[72] Lazaridou M (n 18) 56.
[73] Chidera Okolie, “Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns,” vol 25 (2023) *Journal of Internet Law* https://vc.bridgew.edu/cgi/viewcontent.cgi?article=3079&context=jiws 28.
[74] Salter and Wong (n 68) 22.
[75] Fletcher (n 41) 59.

society.[76] In sexual offences, the protected interest is often the sexual autonomy and bodily dignity of the victim.

But with AI-CSAM, there is often no identifiable individual interest is infringed. Some argue this precludes criminalisation altogether. However, Lazaridou contends that the protected interest is not only the individual child but also "the institution of childhood as a legal and social construct".[77] In this view, distributing AI-CSAM undermines societal values, sexual norms, and the categorical imperative that children should never be sexualised.

The criminalisation of AI-generated CSAM can also be grounded in what Jurasz and Barker described as the "digital sexual integrity of the community".[78] Just as image-based sexual abuse violates the shared expectation of bodily and visual privacy, AI-generated CSAM erodes the collective commitment to protecting childhood from sexual objectification. The UK Law Commission's 2021 report on communication offences similarly emphasise that criminal sanction should shift from "content-based rules" to "actual-harm based rules" focusing on whether the likely audience would suffer harm, rather than on vague categories such as 'offensive' or 'indecent'.[79] This method is similar to Feinberg's expressing concept of retribution, which says that laws are meant to reinforce community ethical norms for punishing people.[80] So, even if there is no direct injury or purpose, breaking a firmly held permitted attraction, like the sexual indestructibility of infancy, could be enough to get you in trouble with the law.

The emergence of AI-generated sexual material is putting the traditional ideas of damage, intention and authorized curiosity to the test. These concepts are still important for a cohesive system of criminal law, but they have big gaps when they are used in digital settings. In cases of sexual offenses that use synthetic images, damage might have genuine however inverse, desire might become shared however still guilty, and legal desires might become shared instead of a someone. As new methods change the lines between right and evil, criminal law must

[76] Feinberg (62) 36.
[77] Lazaridou (18) 60.
[78] Jurasz O and Barker K, "Sexual Violence in the Digital Age: A Criminal Law Conundrum?" (2021) http://oro.open.ac.uk/78691/1/Jurasz%20Barker_Sexual%20violence%20in%20the%20digital%20age%20a%20criminal%20law%20conundrum%20%282021%29.pdf 204.
[79] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 21 July 2021) 25–26.
[80] Feinberg (n 62) 401.

improve its ideas so that it can deal with these problems without losing accuracy or moral honesty.

3. What Constitutes a Crime in the Context of AI-generated CSAM?

This part wants to look at the main question of which makes something a crime, using the criminal law ideas which possess currently become discussed. It looks at why distinctive hypothetical structures think about criminal behaviour. This study not only sheds insight on the philosophical basis for criminal culpability, but it also provides a standard way to look at novel problems, including AI-generated content that involves child sexual assault. It is important to define crime because it affects the types of questions this thesis asks and the sequence in which we look at things.[81] Retributivist theory says that crime involves breaking a moral duty, and the act of committing a crime is worthy of retribution just since it is wrong. That viewpoint says that the criminal's guilt pertains prior to the crime's results.[82] But when it involves AI-generated CSAM, in which no actual kid might get hurt, the ethical ground for retribution grows less evident. On the lack for a direct the target, can the desire to generate replicated exploitation warrant governmental revenge? This question shows the limits of intent-based arguments and makes the revengeful reaction more difficult while a behaviour doesn't have an instantaneous, visible effect.

Essential methods offer a deterministic opinion, which says which activities could be outlawed if they make society as a whole better off. From this point of view, retribution may become defended by reasons that refer to the future, such as discouragement, impairment, and recovery. A pragmatic would say that the existence and spread of AI-generated CSAM would make cruel desires seem usual, increase the market for real child abuse substance, and encourage bad subcultures, even if no one is directly hurt.[83] The law could stop more misuse by making it harder to make and sell fake CSAM. But this paradigm raises tough questions about hypothetical harm, such what level of risk should be enough to make something a crime?[84]

---

[81] Ronald C. Kramer, "Defining the Concept of Crime: A Humanistic Perspective" (1985) *12 The Journal of Sociology & Social Welfare* https://doi.org/10.15453/0191-5096.1715 2.
[82] Moore (n 53) 182.
[83] Bracket Foundation, "Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse" (2024) https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf 17-20.
[84] Bentham, J. & Jonathan Bennett. (2017). *An introduction to the principles of morals and legislation*. https://www.earlymoderntexts.com/assets/pdfs/bentham1780.pdf

The expressivist concept of punishment is a good supplement to these other common ideas. Feinberg[85] and Duff[86] say that criminal law not only punishes people, but it also shows that society disapproves of their actions. This view says that punishment is an act of defiance that shows what is right and wrong. So, it is possible to make AI-generated CSAM illegal to show that sexualizing minors, even if it is not real, is wrong, also when any kid is hurt. Reiterating the values that bring people together is far more essential compared to merely punishing people.[87]

From this expressivist point of view, feminist criticisms that ask who is harmed and who does not come easily. For a long time, feminist criminologists like Carol Smart have said that conventional criminal law often ignores the fundamental and visual abuse which women and children face. When it comes to AI-generated CSAM, the picture and idea of girlhood itself might be used instead of a specific kid. This kind of information helps keep a male-dominated structure of sexual domination going and adds to a larger digital culture that treats children, specifically girls, as objects and something to be bought and sold.[88] Feminist philosophy expands the idea of victimization above the person by looking at damage for groups and cultures.

Ronald C. Kramer's humanistic criminology provides a potent unifying viewpoint to bring the disparate insights of these theories together. Kramer offers two different ways to define crime: first, as a socio-legal construct, and second, as deliberate harm to society. The state defines crime through laws that reflect political will rather than moral truth, according to the first tier.[89] This emphasises how challenging it is to rely only on current legal frameworks, particularly when they are out of step with technological developments. His theory is most innovative at the second level, which views crime as intentional social harm. It challenges criminologists to find destructive behaviours that may not be legally recognised yet but nevertheless compromise social trust, human dignity, and the welfare of the community.[90]

[85] Feinberg (n 62) 400.
[86] Duff (n 70) 56.
[87] Lazaridou (n 18) 60.
[88] Jessica Stratton and Anastasia Powell, 'Digital Criminology: Rethinking Crime in the Online Age' (2021) 17 *International Journal for Crime, Justice and Social Democracy* https://www.crimejusticejournal.com/article/view/865 5.
[89] Kramer (n 81) 67.
[90] Ibid 69

From this perspective, AI-generated CSAM becomes a paradigmatic example. The deliberate production of synthetic sexualised images of children, even in the absence of physical abuse, is a violation of the social duty to protect children and a symbolic assault on the moral standing of childhood. Kramer's framework justifies criminalising AI-generated CSAM not because the law prohibits it, but because it causes significant social harm that ought to recognise as criminal.[91]

Theories of preventive justice, which build on Kramer's normative framework, highlight the role of the law in reducing predictable risks. AI-generated CSAM can be interpreted as anticipatory harm, since its widespread circulation often increases the likelihood that more extreme forms of exploitation will be committed.[92] Therefore, making such content illegal has a preventative effect: addressing the danger before further harm materialises. According to this logic, the state does not need to wait for actual victimisation when credible indicators of risk are already present.

Restorative justice, on the other hand, frequently tries to fix the connection among the victimized and the perpetrator, that is a problem when the victim is not clearly evident. But we can change this idea to fit this scenario. Rehabilitative structures might focus on fixing broken cultural relationships and making up for any damage done for those in danger, especially kids who are figuratively attacked. The crime goes toward the ethical core of culture; thus, it needs more than just reparation; it requires acknowledgment, transparency, and recuperation.[93]

Feminist and online criminology scholars contribute for such discussion through saying that criminal activity in the digital era makes us rethink what it means to be a victim and what it means to have autonomy. Stratton and Powell, for instance, offer a "the internet criminology" that breaks down the false boundary among damage that happens online and damage which happens offline. They say that virtual worlds are a big part of interactions and can have real-world effects.[94]

So, legal terminology by itself isn't enough with determining criminality when it applies with AI-generated CSAM. It needs a whole plan that includes feminist criticisms for strength and participation, practical goals of discouragement, expressivist communications of acceptable

[91] Ibid 69.
[92] Bracket Foundation (n 83) 13.
[93] ibid.
[94] Stratton and Powell (n 89) 5.

behaviour, retributivist worries regarding blame, and Kramer's appeal over ethical responsibility grounded in respect for others. It multidisciplinary approach was the sole means for criminal law to adequately deal with new and complicated damages that threaten the ethical foundation of online the community.

4. Who is Considered the Victim of a Crime?

This part moves away from moral and prophylactic reasons for punishment and asks a more difficult but important question: Who is the victim? In the past, traditional legal theory has generally defined the victim as the person who is hurt in a way that is clear and immediate, either physically or financially. But when it comes to AI-generated kid involving child sexual abuse (CSAM), this restricted view doesn't seem to be enough. Retributivist concepts mostly look upon the criminal's leave along with ethical guilt, leaving the victim in a peripheral role. Later critics, like Fletcher's, pointed out why this kind for conceptualization hides the truth of experienced injury.[95] However, theorists like Jean Hampton have not fully explored the idea of bringing the victim back into the moral justification of punishment by seeing punishment as a way to restore morality in situations where injury is symbolic, anticipated, or figurative.

Utilitarianism, similarly, frames the victim largely as a unit in a cost-benefit analysis. Here, the individual's suffering becomes data in evaluating future deterrence or rehabilitation. This can render invisible the harms experienced by those affected by AI-generated CSAM, such as children whose images were scraped for training data or whose likeness was morphed without their knowledge -individuals who are not easy to quantify but whose suffering is real nonetheless.[96]

Communicative concepts, especially those established by Duff, give another way to look at retribution. They see the act as an opportunity to show that the victim is morally valuable and to restate society's common ideals.[97] From this point of view, the victim is important not only because they were hurt, however because they have ideals that ought to be recognized when they are broken. Finlay extends this idea by saying that retribution may bring the community's ethical fabric back together, rather than for bringing people together, however, through

[95] George Philip Fletcher, 'The Place of Victims in the Theory of Retribution' (1999) 3 Buff Crim L Rev 51.
[96] Bracket Foundation (n 83) 4-6.
[97] Duff (n 70)

sustaining collaborative standards. This is especially important in diverse cultures when ethical agreement is broken.[98]

Prevention concepts usually emphasize lowering potential risks instead of fixing previous damage, yet this doesn't imply the victim goes away.[99] As an illustration, Andenaes said that for the criminal law to stay valid, injury must be real and apparent for the public. This made the victim an image of mutual danger and social cohesiveness. Recovery justice, upon the contrary, puts the victim at the centre and encourages them to take an active role in the justice process, not just as a beneficiary but also as a repair agent. This is particularly relevant in AI-CSAM scenarios, which typical algorithms can't find a "real" victim, but therapeutic techniques may involve people who suffer injury indirectly as well as a way that represents the victim.[100]

Feminist criminal law, upon the other hand, asserts that the idea of a victim is structured and sexist. Crenshaw's idea of interconnection says that gender, racism, and social classes make certain populations more vulnerable, particularly women and girls online. Carol Smart and Meda Chesney-Lind say which being a victim isn't merely the result of a crime; it is also a sign of bigger cultural structures which decide whom it is worthy of legal acknowledgment.[101] This way of thinking is important in situations of AI-generated CSAM, which the damage is often figurative or indirect but intimately tied for the fact that children, especially girls, are seen as online products.

There are additionally others who don't like the term "victims." Pease has said that calling an individual a victim may take away their authority and reinforce stories of reliance, inaction, and feeling powerless.[102] The change for naming those who have been hurt "survivors" is meant to give them back their power and strength. A shift in language, on the other hand, may occasionally times hide underlying inequality and ignore fewer apparent types of suffering, such figurative and loss of credibility. Cassell and Morris say which the law ought to define

---

[98] Jonathan Doak, 'Defining Victim Through Harm: Crime Victim Status in the Criminal Process' in Matthew Hall, Joanna Shapland and Julian V Roberts (eds), *Victims of Crime: Problems, Policies and Programs* (2nd edn, Palgrave Macmillan 2021) 159.
[99] Kramer (n 81)
[100] Kokolaki V, 'Digital Harm and Victimhood in the Context of AI-Simulated Abuse' in *Sexual Violence in the Digital Age* (Springer 2021) 197–198.
[101] Chesney-Lind M and Pasko L, *The Female Offender: Girls, Women, and Crime* (2013) https://doi.org/10.4135/9781483387567
[102] Ken Pease, 'Victims and Victimization' in Shlomo Giora Shoham, Paul Knepper and Martin Kett (eds), *International Handbook of Penology and Criminal Justice* (CRC Press 2007) https://islingtoncrimesurvey.wordpress.com/wp-content/uploads/2016/02/2007_victims.pdf 587.

"victim" in general as everyone who is "immediately and closest damaged" by a crime.[103] This broad threshold gives the law a way to recognize the damage done to people whose resemblance are used by AI systems to make fake exploitation material, regardless of whether they weren't the main victims. Kleinfeld backs up this idea by saying that being a victim must show morally important differences, such the difference between hurting an agreeing mature and a kid, or among attacking a criminal and a weak citizen. This is quite important when it comes to AI-generated CSAM, because the fake injury typically has to do with children's social groups and significance in society instead of their physical appearances.[104]

Finally, by pointing out morally important traits of the victim, Kleinfeld shows a major flaw in traditional criminal theory. He says that ignoring things like age, innocence, or social vulnerability makes it impossible for a legal system to tell the difference between, say, an attack on a gang member and an attack on an innocent kid, or between injury done to a consenting adult and harm done to a youngster.[105] These differences are quite important in circumstances of AI-generated CSAM, when the injury might not seem actual however is nevertheless genuine. The material can seem like actual kids, take advantage of weaknesses in society, or be part of an overall society which makes exploitation seem typical or unimportant. To really comprehend what it means to be a victim, we need to look at more than just the physical suffering. We also need to look at figurative, a metaphor and anticipation harm. In this case, asking "who is the victim?" is not only an issue of terminology; it is also a question of norms and politics that questions the basic ideas of criminal law and pushes the limits of what is legally and morally possible.

5. Conclusion

The following section looked that the hypothetical basis for criminal law and showed how standard ideas don't hold up well while experienced with AI-generated child assault materials. Damage, purpose, and victimhood are conventional foundations of criminal law, but they are becoming decreasingly useful when it comes for manufactured offenses wherein there are no real sufferers, no actual wounds, no conventional performers. Retribution concepts, whether

[103] Paul G Cassell and Michael R Morris, 'Defining "Victim" through Harm: Crime Victim Status in the Crime Victims' Rights Act and Other Victims' Rights Enactments' (2024) *Utah Law Faculty Scholarship* https://dc.law.utah.edu/scholarship/392/ 12.
[104] Joshua Kleinfeld, 'A Theory of Criminal Victimization' (2013) 65 *Stanford Law Review* https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2013/06/Kleinfeld_65_Stan._L._Rev._1087.pdf 1087, 1092–1096.
[105] Ibid.

they are harsh, practical, or therapeutic, each provide us some useful information, but they need to be changed to deal with the figurative and planned harms that are built into electronic depictions. This section has highlighted how criminal law has to change to be relevant in a technology era by using feminist, expressive, and preventive frameworks. This section further shows that AI-generated CSAM needs an enforceable overhaul that goes beyond models of damage and blame that focus on people. As criminal law struggles to draw clear borders among fictitious and abuse, it is becoming increasingly important to have an analytical structure that can detect figurative assault and structure victimhood.

CHAPTER III: AI-GENERATED IMAGES

1. What is AI-generated Imagery?

Artificial intelligence has changed a lot how visual material is made in the last few years. Diffraction algorithms (DMs), generative adversarial networks (GANs), and huge multimodal foundation models can now make fake pictures that look a lot like actual photos. "AI-generated imagery" is a phrase for pictures made through structures that have been taught upon enormous data sets from the actual world. Unlike standard computer-generated graphics, those pictures depend upon discovered patterns of statistics which have built into neural connections instead than being made by hand.[106]

The 2 key structures that make that change possible are GANs and DMs. GANs utilize a dual-network topology, with an algorithm for making pictures and an analyser checking for whether they are real. With each educating period, the tool gets better at making accurate pictures that seem like actual ones. On the other hand, DMs take disturbances and turn it into organized pictures through a process called denoising, which makes outputs that are very detailed. These models have done an amazing job of turning messages into pictures that seem like practical problems illumination, framework, and appearance.[107]

Notably, platforms such as DALL·E, Midjourney, and Stable Diffusion enable users to generate images from natural language descriptions. These outputs often reflect both stylistic and contextual knowledge encoded from the training data. As Yu et al. have noted, AI-generated images may either be created from scratch or manipulated from pre-existing visuals -frequently in ways that are difficult to detect without forensic analysis.[108] This dual capacity renders AI tools uniquely capable of both creative experimentation and malicious manipulation.

AI-generated pictures are employed in many fields such as online advertising, games, style, medical treatment, and academic modeling. In artistic fields, they are appreciated for how well they work, how easily they can be scaled up, and how accurately they can be seen. Yet those

[106] Ziv Epstein, Aaron Hertzmann, and Investigators of Human Creativity, "Art and the Science of Generative AI" (2021) journal-article https://ide.mit.edu/wp-content/uploads/2023/07/science.adh4451-1.pdf?x76181 1.
[107] Eva Cetinic E and James She , "Understanding and Creating Art with AI: Review and Outlook" (*arXiv.org*, February 18, 2021) https://arxiv.org/abs/2102.09109 2-3.
[108] Xioamin Yu and others, "Fake Artificial Intelligence Generated Contents (FAIGC): A Survey of Theories, Detection Methods, and Opportunities" (2024) https://arxiv.org/abs/2405.00711 3.

same characteristics make me very worried. Opponents say which these kinds of algorithms only mix up old data without making anything new, a process they call "stochastic parroting."[109] They also raise moral issues about authorship, identity duplication, and the loss of creative freedom.

AI-generated images additionally raise questions about what is real and what is not. Is it possible for a picture to be "false" if it seems true however doesn't show an actual occasion? And greater importantly for my thesis, what does it mean when these kinds of pictures show kids in sexual situations, regardless of no real kids are in them? These concerns show how AI-generated images opposition existing laws about purpose, participation, and injury.[110]

In fact, creative AI ushers in a new genre having a variety of opportunities, rather than heralding the "end of art," as pointed out by Epstein et al. The "imaginative behave" changes across producing images with coming up with prompts and defining them.[111] In these kinds of structures, the significance of a photo is not just made for the picture itself, however also by how it is used, understood, and shared.

In short, AI-generated images are greater than just a new technology; they change the way we make, understand, and control pictures material. Its strength comes from how genuine it is, but its danger comes from how unclear it is, especially when used in morally questionable areas like synthetic CSAM. So, a whole legal and intellectual answer must look at not just how these pictures are generated, additionally which they mean, who they influence, and how they move around in the online world.

2. Legal Status of AI-generated Images

Because AI-generated photos don't have a real human's creator or bound, their constitutional standing is still quite unclear within many places. The absence of clarity in the justice shows that it's hard to make sense of how current rules apply to inhumane agents. AI-generated material covers a wide range of topics, from art to fake media that looks like people. However,

[109] Emily M Bender and others, 'On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?' (2021) *FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* https://dl.acm.org/doi/10.1145/3442188.3445922 1.
[110] Epstein et al. (n 108) 1-2.
[111] Ibid.

when such material shows delicate topics like minors in sexualized situations without showing real people, it makes it even more difficult to hold someone criminally responsible.

The General Data Protection Regulation (GDPR) in the European Union says that you can't the procedure private information, such biometric information data and facial likenesses, lacking a good reason or permission. Although artificial pictures might not depict real people, artificial intelligence platforms that are taught on material that has been extracted about the internet might accidentally duplicate recognizable traits or representations, which can cause damage in other ways.[112] The GDPR's structure doesn't make this problem apparent, and implementation typically delays behind technical progress.

The European Union's Artificial Intelligence Act also tries to control high-risk AI structures, especially individuals that use biological identity or deceptive methods. paragraph nine of the legislation fails to declare photo production a crime; however, this recognizes the possible dangers about artificial intelligence structures which mimic people or alter data in manners that might be misleading or harmful to mental health.[113] This is important for AI-generated CSAM since it may look like illicit material lacking mentioning real kids. However, it might also make abusive depictions seem natural and go against child protection norms.

AI-generated CSAM is hard to regulate since traditional criminal law frequently needs a genuine victim to prove damage. A few nations like the UK and Australia, make it illegal to show fictitious portrayals of child sexual abuse. Other others, like portions of the US, need the presence of a real kid. This difference creates legal gaps that make it harder to stop the spread of items that are harmful. Scholars say that a simply harm-based strategy is not enough. Instead, they say that symbolic and preventative forms of criminalization should be used to deal with figurative and societal damage.[114]

proactive structures say which criminalization is okay if there is a high chance of damage happening in the future, including grooming, desensitization, or the use of fake information to make children more sexualized. This makes sense alongside the EU's focus on human-centred

[112] 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 (General Data Protection Regulation) [2016] OJ L119/1, recital 9. https://www.privacy-regulation.eu/en/recital-9-GDPR.htm

[113] EU Artificial Intelligence Act https://artificialintelligenceact.eu/

[114] Rafael Dean Brown, 'Property Ownership and the Legal Personhood of Artificial Intelligence' (2021) 30(2) Information & Communications Technology Law https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746768 21-22

and reliable artificial intelligence, which says which should be built with responsibility, openness, and basic rights in mind. Still, there are still gaps in the law, notably when it comes to artificial intelligence (AI) platforms that are made and used in several countries, frequently without GDPR regulation.

Discussions across when artificial intelligence ought to become given juridical status add a different level for complexities. Several people say which giving artificial intelligence limiting permitted personality, like companies, could make rules clearer and make people more responsible. Critics, on the other hand, say that legal personality calls for independence, deliberateness, and moral agency, which AI systems do not have. Koos says that artificial intelligence ought to only be legally recognized if it meets the requirements of human participants and is rather than based on an inherent right to rights.[115]

Marshall goes farther with this criticism stating it's too soon to talk about AI rights, especially as civil rights safeguards over previously excluded people are still not finished. She warns toward giving code-based structures legitimacy when human rights laws are still not being implemented enough. She says that giving AI legal personality might make current inequities worse in the digital world.[116]

Finally, the question of how to treat images created by Intelligence in a judicial context is far from settled. As more and more pictures information is made by machines and doesn't have anything to do with real life, the law needs to change primarily for keep out with advances in technology however additionally for keep up with changing ideas about damage, participation, and autonomy. Those contradictions have been specifically strong when it comes to protecting children and stopping online abuse, when the meaning of a picture could extend beyond what the law now allows. the structure of the law more logical, it might be necessary for broaden the ideas that make up criminal law to include manufactured damages that have real-world effects.

3. What is AI-generated CSAM?

AI-generated child sexual abuse material (AI-CSAM) is a type of computer-generated image that shows kids in sexual situations. Those pictures aren't for actual kids taken with a camera

[115] Stefan Koos, 'A Normative Framework for Artificial Intelligence: Between Legal Subjectivity and Regulatory Instrumentalism' (2023) 5(1) *Technology and Regulation* https://doi.org/10.33102/mjsl.vol6no3.135 4.
[116] Brandeis Marshall, "No Legal Personhood for AI" (2023) 4 Patterns 100861 https://doi.org/10.1016/j.patter.2023.100861 1-2.

along with video camera. Instead, they were made through methods that were taught upon huge amounts for information. Thiel shows which records like LAION-5B, which are often utilized to train machine learning models, contain identified or reported CSAM. Thus, the results are subsequently based on real exploitation substance.[117] The Internet Watch Foundation also points out that artificial intelligence may make completely new but very realistic images of child abuse without even mentioning a specific child.[118]

AI-CSAM questions traditional ideas of who is a victim and who is a criminal, even when no recognizable kid may show in the output. Its realism, ease of use, and potential to change create severe moral and mental health issues. Scholars have pointed out that it might make dangerous urges seem normal, make users less sensitive for harassment, and keep abusive figments going.[119] Also, there is still a lot of legal uncertainty in many places, especially while the material is made "from scrape" and doesn't directly mention a real child.[120] Nevertheless, politicians are starting to realize how dangerous AI-CSAM is, which is leading to proposals for regulation based on expressed and preventative equity.

The emergence of AI-generated CSAM (AIG-CSAM) challenges established legal, psychological, and normative frameworks. Such content is created by generative AI models, such as diffusion models or GANs, that may produce photorealistic or stylised images of children in sexualised scenarios. Some AI-generated images are based on scraped real-world data, including known CSAM, while others are produced entirely from user prompts, yet evoke recognisably exploitative imagery. The realism, accessibility, and customisability of these synthetic depictions have introduced new vectors for harm, desensitisation, and abuse fantasy reinforcement.[121]

Legal responses vary considerably across jurisdictions. Some countries, like the UK and Australia, criminalise fictional depictions, including cartoons and morphs, while others,

---

[117] David Thiel, Leah Stroebel and Rebecca Portnoff, *Identifying and Eliminating CSAM in Generative ML Training Data and Models* (Stanford Internet Observatory, 23 December 2023) https://stacks.stanford.edu/file/kh752sm9123/ml_training_data_csam_report-2023-12-23.pdf 10.
[118] IWF (n 69) 4.
[119] Kara Struckman, 'Combatting AI-Generated CSAM' (Wilson Center, 27 November 2023) https://www.wilsoncenter.org/article/combatting-ai-generated-csam accessed 2 July 2025.
[120] Cézanne Van den Bergh, "AI's Chilling Impact on Child Sexual Abuse Material: A Wake-up Call for the International Community - Global Campus of Human Rights" https://www.gchumanrights.org/preparedness/ais-chilling-impact-on-child-sexual-abuse-material-a-wake-up-call-for-the-international-community/ accessed 2 July
[121] Thiel (n 117) 2.

including parts of the US, require the involvement of an identifiable child to meet statutory definitions of CSAM.[122] This discrepancy has generated significant concern among child protection advocates, who argue that AI-generated CSAM, even if technically "fictional," may foster grooming, erode societal taboos, and circulate among offenders as a replacement or precursor to real abuse.[123]

To better conceptualise the types of AI-generated CSAM, legal scholars and practitioners have proposed typologies based on production method and degree of connection to real individuals. The three most frequently cited categories are morphed, photorealistic, and abuse-trained CSAM.

a. Morphed CSAM

Morphed CSAM is when a genuine child's face or other identifying features are online combined alongside the physical features about an adult or a fake person in a sexualized way. These photographs commonly originate about accessible internet accounts. Even if no bodily exploitation happens during the making of these pictures, they look like exploitation and might hurt the child's mental health and image.[124]

Some laws, like the UK's Protection of Children Act 1978[125], recognize the symbolic power of representation. This law was changed by the Criminal Justice and Public Order Act 1994[126] to cover indecent "pseudo-photographs" even when no real kid is involved. Pfefferkorn says that morphing technologies make it harder to tell the difference between fiction and reality in bad ways, because they use actual identities to pretend to be exploited. This is a reason to make it illegal for both expressive and preventative reasons.[127]

Making altered CSAM makes it hard to tell the difference among communication and abuse, especially if an image of the kid is used without permission. Researchers say which using a

[122] Struckman (n 119)
[123] IWF (n 69) 5.
[124] Thorn, 'What is CSAM? Child Safety Terms & Definitions' (2025) https://safer.io/resources/common-terms-and-definitions/.
[125] UK Protection of Children Act 1978 (n 39) s 1(1)
[126] Criminal Justice and Public Order Act 1994 s 84(4) https://www.legislation.gov.uk/ukpga/1994/33/section/84
[127] UK Protection of Children Act 1978 (n 39) s 1(1)

child's picture, regardless of touching them, is a type of abuse based on their identity that should be punished by law.[128]

b. Photorealistic CSAM

Photorealistic CSAM is made up of AI-generated photographs of completely made-up kids in very realistic and graphic sexual situations. Text-to-image dispersion algorithms which might turn stated suggestions onto high-quality images have been commonly used to make these. Even though they don't include any actual child, they can seem almost exactly like genuine abuse substance and are routinely discussed in the same groups of offenders.[129]

Offenders said they like AI-generated photos better because they think they are "legal," can be changed, and are tougher to find.[130] Pfefferkorn says that this false sense of legitimacy is what allows more exploitation to happen, as criminals utilize it to avoid being held accountable while still doing things that cause harm.[131]

These images may contribute to desensitisation, reinforce abuse scripts, and create demand for actual CSAM. Their legal status remains ambiguous: while some jurisdictions outlaw "prohibited images" regardless of origin, others protect such images as free speech in the absence of an identifiable victim.[132]

c. Abuse-trained CSAM

Abuse-trained CSAM, which are fake pictures made for artificial intelligence systems which have been taught on genuine CSAM datasets, is perhaps the majority morally and legally troublesome type. Thiel says that huge picture datasets like LAION-5B, which are used to train models like Stable Diffusion, have been discovered to have known and suspected CSAM in them.[133]

---

[128] Criminal Justice and Public Order Act 1994 s 84(4) https://www.legislation.gov.uk/ukpga/1994/33/section/84
[129] Pfefferkorn R, 'Addressing Computer-Generated CSAM: A Normative and Legal Framework' (2024) https://s3.documentcloud.org/documents/24403088/adressing-cg-csam-pfefferkorn-1.pdf 5-6.
[130] Van den Bergh (n 120)
[131] Thiel (n 117) 3.
[132] Thorn (n 127) 3.
[133] Thiel (n 117) 2-3.

Even yet the results might be fake, they are based on genuine exploitation substance, which raises issues of derived victimization. Pfefferkorn says that education on CSAM is not just a technological problem yet a moral one that recreates the harmful effects of exploitation while no real kid is displayed.[134]

This approach is a cyclical threat: when examples taught upon cruel information have been utilized for make additional material, criminals can keep making and improving photos which demonstrate how exploitation happened in the past. These models might make it easier to make exploitative images while hiding where they came from, making it harder to find and hold people accountable.[135]

CSAM goes against some of the most basic ideas in criminal law, especially the idea that damage and victimization are connected. Those pictures, how they have been altered, accurate, for abuse-trained, may all make exploitation seem genuine, bring up exploitation stories, and have ramifications that go beyond the law, psychology, and morality. These sections may talk about the way constitutional frameworks have been changing to deal with new dangers, or not at all.

4. Conclusion

This section talks about the technological and legal aspects of Artificial Intelligence images, with an emphasis on how they can be used as weapons for the purpose of sexually assaulting children substance. As has been shown, the realism and flexibility of AI-generated material have broken down long-standing legal and moral barriers, especially when no real kid is directly engaged. Looking at customized, photorealistic, and exploitatively trained CSAM shows that even fake content may hurt people mentally, socially, and in terms of their future, and this is frequently more than what is allowed by law if there is a clear victim. These documents are not clear, which makes it harder for the police and child protection services to do their jobs. They also show how important it is to rethink the limits of criminal law in light of representative harm.

Also, the types of abuse discussed in this chapter show that binary legal categories (genuine and false, victim and no victim) don't work well for dealing with the intricacies of synthetic

[134] Pfefferkorn (n 129) 6-7.
[135] IWF (n 69) 18.

abuse. Existing laws typically don't include synthetic material because they don't include it in legal definitions or because they don't think about all the different ways it might hurt people. So, this chapter sets up the following one, which looks at how both domestic and international legal systems have started to deal with the growing threat of AI-generated CSAM, even if they haven't done a very good job of it yet.

CHAPTER IV: LEGAL REGULATIONS AND GAPS

1. Current Legislation

a. International Law and Soft Law Instruments

The worldwide structure for dealing with child sexual abuse material (CSAM) possesses changed a lot because of the rise of online dangers. Those tools were first created to deal with classic types of exploitation, but today they have been used with deal with new types about manufactured and AI-generated CSAM. Yet, even if there were a few positive changes, especially that the EU stage, the situation was nonetheless dispersed for a time, about problems alongside definitions, authority, and regulation.

he Court of Europe's Lanzarotte Convention (2007)[136], the Budapest Convention on Internet crime (2001)[137], and the Additional the Agreement for the Convention on the Child Rights of the Child (OPSC)[138] are all examples of global constitutional documents that provide basic foundations. Under Article 20 of the Lanzarotte Convention, it is against the law to make, own, or share "any representation of a child engaged in real or simulated sexually explicit conduct." But Article 20(3)[139] lets parties leave out virtual child pornography if "no real child was used." This means that signatory governments can avoid criminal charges for AI-generated CSAM even when it looks a lot like genuine exploitation.

Similarly, the OPSC focuses on “the sale of children, child prostitution and child pornography,” but its definitions traditionally assume the involvement of real children. Interpretive declarations and state practice have consistently limited its application to abuse involving identifiable minors.[140]

[136] Pfefferkorn (n 129) 6-7.
[137] IWF (n 69) 18.
[138] Council of Europe, *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)* (adopted 25 October 2007, entered into force 1 July 2010) CETS No 201 https://rm.coe.int/1680084822 accessed 3 July 2025.
[139] Council of Europe, *Convention on Cybercrime* (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185 https://rm.coe.int/1680081561 accessed 3 July 2025.
[140] OPSC (n 14) Art(2)

The Budapest Convention's Article 9 criminalises child pornography online but likewise lacks specific provisions addressing AI-generated or synthetic abuse material. According to Kolen, this omission reflects a conceptual and technological lag in international cybercrime legislation, though negotiations for a second protocol are underway to address novel digital threats.[141]

A more dynamic approach has emerged within the European Union Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children explicitly includes "realistic images" within its scope, allowing for AI-generated photorealistic CSAM to be criminalised even in the absence of a real child. However, the directive leaves implementation to the discretion of member states, and transposition remains uneven.[142]

The European Committee had suggested a Redefining of Regulation 2011/93/EU to fix problems with it. The new phrasing makes it illegal to show "feasible or manufactured illustrations" for minors, while it expressly specifies AI-generated material as part of this.[143] This gives all EU countries a common constitutional definitions for CSAM and tries to close any gaps in the law by making sure that the way the law treats CSAM is in line alongside how it is used today, such as through changes, counterfeits, while manufactured material. Additionally, it suggests better help over sufferers while better collaboration across borders.[144]

The European Union's AI Regulations (2024)[145] makes things clearer by saying kids are a susceptible category beneath paragraph 28a.[146] This provides this by quoting either the Commentary No. 25[147] for the United Nations Protocol on the Legal Rights of a Children

[141] Kolen E, "A Modern Tale of Frankenstein?: How to Regulate Non-Consensual Sexually Explicit AI-Generated Deepfakes in the Metaverse" (2024) 5.
[142] Directive 2011/93/EU (n 37)
[143] Kolen E (n 141) 5.
[144] Directive 2011/93/EU (n 37)
[145] European Parliamentary Research Service, *Criminalisation of Gender-Based Violence against Women: State of play and legislative developments in view of the Istanbul Convention and the proposed EU Directive on violence against women and domestic violence* (Briefing, PE 762.374, June 2024) https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762374 accessed 3 July 2025.
[146] INHOPE, 'How the Recast EU CSAM Directive Empowers INHOPE Hotlines' (INHOPE, 2024) https://inhope.org/EN/articles/how-the-recast-eu-csam-directive-empowers-inhope-hotlines accessed 3 July 2025
[147] "EU Artificial Intelligence Act | Up-to-Date Developments and Analyses of the EU AI Act" https://artificialintelligenceact.eu/ accessed 3 July 2025.

(UNCRC)[148] and Section 24 within the Constitution of Essential Liberty.[149] The legislation makes extremely dangerous artificial intelligence follow rigorous rules along with be open about what they perform, but it doesn't say that AI-generated CSAM is illegal.

There are still worries about how the Artificial Intelligence Act will be enforced. national regulatory bodies have the charge of making sure that rules are followed, however a lot of them don't have the tools to find or analyse AI-generated material, especially if the material is made using decentralized or publicly available theories. Also, the lack of a single stating or responsibility system makes it harder for countries to work together across borders.[150]

The General Data Protection Regulation (GDPR)[151] protects genuine kids records in a way that is similar to how criminal laws protect it. paragraph 71[152] and Article 22[153] of the GDPR, on the other hand, are mostly about analysing and rendering decisions automatically about real people. It might not include fictitious or manufactured depictions that don't have recognized information topics regardless of whether their seem such as real kids who were taken from open documents.

Smooth legal tools possess additionally helped in other ways. The UN's general observations No. 25 on the protection of children in the online world stresses how important it is to keep kids safe from new dangers, such as making and changing images without their permission.[154] The United States Special Rapporteur on the Sale and Abuse of Children has also talked about how important it is to amend the law's definitions for damage, victimization, and abuse to include substance produced by artificial intelligence.

[148] "Recital 28 | EU Artificial Intelligence Act" https://artificialintelligenceact.eu/recital/28/ accessed 3 July 2025.
[149] UN Committee on the Rights of the Child, *General Comment No 25 (2021) on children's rights in relation to the digital environment* (2 March 2021) UN Doc CRC/C/GC/25 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation accessed 3 July 2025.
[150] Koos (n 115) 7.
[151] European Parliament, Council of the European Union, and European Commission, "CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION" (2000) report https://www.europarl.europa.eu/charter/pdf/text_en.pdf Art 24.
[152] Koos (n 115) 7.
[153] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng accessed 3 July 2025.
[154] GDPR 2016, recital 71

In short, the global legal system is starting to adjust to changes in technology, but it is not yet fully in line alongside the facts of AI-generated CSAM. Traditional structures, which were based on real-child abuse, have a hard time including manufactured exploitation. The European Union is leading the way in legislative changes with its Redefining Regulation and artificial intelligence Act, but there is still serve with be done for make laws the same throughout the world. To make certain that constitutional systems maintain up with how child sexual exploitation is changing in the online era, we need to constantly be developing, harmonizing, and coordinating the implementation of laws.

b. Legislation and Approach in Europe

The United Kingdom has taken a relatively broad legislative approach to criminalising non-real CSAM, including AI-generated images. Under the Protection of Children Act 1978, The UK possesses made a lot of laws to make it illegal to have non-real CSAM, such AI-generated photos. The Protection of Children Act 1978 says that "inappropriate pictures" for kids involve "pseudo-photographs," meaning pictures who have been online changed or made to seem like actual kids.[155] The Funeral directors and Equity Act 2009 adds further to this by making it illegal to have "banned photos about kids," such as sexually explicit and excessively unpleasant, repulsive, or generally inappropriate pictures focusing on the sexual organs or anal area.[156]

The United Kingdom's Internet Security Act 2023 adds additionally ways towards keep tools responsible. This mandates assistance suppliers utilize material caution and surveillance tools, such as for CSAM that is not a picture or was made by artificial intelligence. But although making internet providers more responsible, this doesn't change what kinds of things are illegal.[157] The Internet Watch Foundation (IWF) has the capacity with send notifications and demands for taking lower accurate artificial intelligence material that it thinks is CSAM. If the picture doesn't fit into this category, it can still be considered a "non-photographic banned picture" beneath current illicit laws.[158]

---

[155] GDPR 2016, Art(22)
[156] Coroners and Justice Act 2009 (n 40) s 62.
[157] Online Safety Act Explainer (Department for Digital, Culture, Media & Sport, 2024) https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer accessed 3 July 2025.
[158] INHOPE, "Global CSAM Legislative Overview" (Second, 2024) https://inhope.org/media/site/e3bb326ed7-1729001643/global-csam-legislative-overview-2024-full-report.pdf accessed 3 July 2025.

The United Kingdom the Sentence Council's punishment recommendations tell judges with think about how realistic and harmful manufactured material is when deciding who is guilty. This shows that the judiciary recognizes figurative damage to AI-generated images. The United Kingdom's laws about AI-generated CSAM are some of the most open in Europe, although there are still problems with regulation, like showing desire or reality.[159]

Germany's laws against child sexual abuse material are mostly found in Chapter 184b of the German Criminal Code (StGB).[160] This section makes it illegal to have, share, or make pornographic material that involves children. The law usually only applies to materials that shows real children, and it doesn't say anything about synthetic or AI-generated stuff. Because of this, it's still not apparent if this requirement applies to CSAM that is only virtual or made by AI.[161]

The German Federal Criminal Police (BKA) started a contentious regulation in 2021 that allowed the deployment of manufactured CSAM made with deep-fake technologies in surveillance missions to find and catch internet criminals. These items weren't rather than to be shared; they seemed meant to be used as lures over an investigation.[162] Since officials justified the procedure on functioning reasons, opponents expressed worries regarding the constitutionality and morality of state-generated abuse pictures, particularly given the lack of obvious legislative permission. There is a legal grey area since the criminal Code does not clearly say that police implementation isn't responsible over making like substance.[163]

The use of these kinds of fake photos by state officials shows a strange legal contradiction: whereas private citizens can be charged with making or having such materials, law enforcement can employ investigatory need without a legal foundation. The law or the courts have not yet been able to fix this problem.[164]

---

[159] Sentencing Council, *Response to Consultation: Sexual Offences Guidelines* (Sentencing Council, 2022) https://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Response_to_Consultation_web1.pdf accessed 3 July 2025.
[160] *Strafgesetzbuch* (German Criminal Code, StGB), § 184b https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1902 accessed 3 July 2025.
[161] INHOPE (n 158) 157.
[162] The Next Web, 'German investigators to use deepfake images of child sexual abuse to bust online predators' (TNW, 26 August 2021) https://thenextweb.com/news/german-investigators-to-use-deepfake-images-of-child-sexual-abuse-to-bust-online-predators accessed 3 July 2025.
[163] INHOPE (n 158) 159.
[164] Koos (n 115) 7.

The Netherlands possesses a constitutional system that is quite innovative yet not yet full when it comes to AI-generated CSAM. Article 240b of the Dutch Criminal Code makes it illegal to make, share, or own all imagery which "seems for indicate an individual who is young" in a sexual context.[165] It involves sketches, visuals, and fake stuff that looks like kids, additionally if there aren't any genuine kids around.[166]

The Dutch the legislature enacted changes in October 2024 to make it clear which the legislation remains in effect additionally when the individuals shown is not real and looks like a youngster.[167] That change makes the law clearer, but there are still certain circumstances where it's not clear what the law means when it comes to entirely AI-generated pictures that don't look such as people or have physiological realistically. Since 2025, the courts still haven't set a clear standard for why for handle such instances, especially while it's hard to demonstrate intention and injury.[168]

The Netherlands has also faced criticism for being a major host of CSAM content due to its advanced data infrastructure and limited content takedown requirements. The Internet Watch Foundation (IWF) has consistently listed the country among the top locations for CSAM hosting, despite national efforts to modernise the criminal code.[169] According to the Dutch intelligence service (AIVD), this issue extends beyond legal reform and requires infrastructural and international coordination.[170]

Sweden has long maintained a strict and appearance-based approach to child sexual abuse material, criminalising not only content involving real children but also fictional or synthetic representations. Under Chapter 16, Section 10a of the Swedish Penal Code,[171] it is a criminal offence to depict minors in pornographic images, regardless of whether the image is

---

[165] Dutch Criminal Code (Wetboek van Strafrecht), art 240b https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Netherlands-Criminal-Code.pdf accessed 3 July 2025.
[166] INHOPE (n 158) 209.
[167] Bert Hubert, 'Dutch Intelligence Service (AIVD) on CSAM: Update and Concerns' (2024) https://berthub.eu/articles/posts/dutch-intel-service-csam-update/ accessed 3 July 2025.
[168] INHOPE (n 158) 211.
[169] Internet Watch Foundation, *The Online Safety Act (OSA) Explained* (IWF, 2024) https://www.iwf.org.uk/policy-work/the-online-safety-act-osa-explained accessed 3 July 2025.
[170] Hubert (n 167)
[171] Swedish Penal Code, ch 16, s 10a https://www.government.se/4a7ad6/contentassets/c68c6dfce58b4045b6d825ba0a97db4e/the-swedish-penal-code accessed 3 July 2025.

photographic, animated, or entirely computer-generated.[172] The law explicitly covers content where the person "appears to be a child," allowing for the inclusion of AI-generated and cartoon-style material.

This criterion based on looks has been there while at least the late 1990s. It was made stronger by court judgments that said people might be charged with a crime for creating manga-style pictures of fictitious kids in sexual situations.[173] The Swedish highest court has ruled that these rules apply to content that doesn't hurt anybody physically but is thought to help create a culture of misuse and normalizing child assault.[174]

Sweden has one of the harshest laws in Europe, yet there is still a lot of controversy about how far creative freedom may go and how fair it is. Still, its laws are often used as an instance of how metaphorical and figurative damage may be used to demonstrate making something illegal even if there are no real victims.[175]

Chapter 311 of Norway's The punishment Code makes it illegal to make, own, or share kids sexually exploitation materials. This includes all pictures portrayal of sexual assault including children.[176] But the legislation doesn't say anything particular about material that is made by artificial intelligence and computers. The permitted means, on the other hand, concentrates on how exploitation the portrayal is lacking saying if fictitious or completely computer-generated pictures are liable.[177]

Norway is legally required to fight child sexual abuse since it signed either the Lanzarote and Budapest Protocols. Still, the country's laws don't currently have any rules that specifically target AI-generated CSAM. if confronting fake material, justice agencies use interpretive theories and look at each case individually.[178]

[172] INHOPE (n 158) 362.
[173] Wired, 'Sweden Sour on Kid Porn' (1 May 1998) https://www.wired.com/1998/05/sweden-sour-on-kid-porn/ accessed 3 July 2025.
[174] INHOPE (n 158) 363.
[175] UNCRC 20210 (n 151) para 79.
[176] Lovdata, *Penal Code of Norway (Straffeloven)*, s 311 https://lovdata.no/dokument/NLE/lov/2005-05-20-28 accessed 3 July 2025.
[177] INHOPE (n 158) 375.
[178] Ibid 376.

Norway is actively involved in international projects like CIRCAMP (the COSPOL Internet Related Child Abusive Material Project), that strives with bring together attempts from different countries to fight via the web CSAM. Taking part in these kinds of projects shows a willingness to work with other European countries, and there might be regulatory changes towards deal alongside new concerns brought through productive technology.

The Lanzarote Protocol while Regulation 2011/93/the European Union are examples of multinational measures that set the beginning requirements throughout the European Union. However, the way those norms are interpreted along with applied to AI-generated CSAM varies greatly from country for country. The differences are mostly due to unclear definitions and the lack of EU-Stage rules that clearly include manufactured sexually depictions of youngsters.[179]

When it comes to national strategies, the UK is among the best detailed.[180] The Security of Children Act 1978 and the Coroners and Justice Act 2009 together make it illegal to have "pseudo-photographs" and "banned pictures" that don't show actual children[181]. The Online Safety Act 2023 has made this stronger through giving tools aggressive duties and giving authorities like Ofcom and the Internet Watch Foundation the right to behave upon manufactured CSAM.[182]

Germany's constitutional situation is less clear. Chapter 184b of the Criminal Code makes it illegal to have CSAM with genuine children, yet it doesn't say anything about manufactured material.[183] But the police's contentious application of AI-generated CSAM in irritate activities shows that there is still some legal doubt about state-created manufactured material. Opponents say that this method does not have an obvious legal exception and might go against the very rules which are supposed for safeguard kids.[184]

The Netherlands, on the other hand, recently changed Article 240b of its Criminal Code[185] to make it clear that it covers pictures of people who "look like they are underage," even if they aren't. This puts the Netherlands ahead of many other jurisdictions, but there are still problems

[179] INHOPE (n 158) 23.
[180] UK Protection of Children Act 1978 (n 39)
[181] Coroners and Justice Act 2009 (n 40)
[182] IWF (n 169)
[183] Strafgesetzbuch (n 160)
[184] Koos (n 115) 7.
[185] Dutch Penal Code (n 165) art 240b.

with execution, especially when it comes to making images look authentic and enforcing takedowns.[186]

Sweden has an enduring norm for criminalizing photographs of children which are actual, lively, or made by artificial intelligence. The law doesn't need verification of the individual's belonging; alternatively, it focuses on figurative injury and societal message.[187] Norway's The punishment Coding makes it a crime to show images of sexual assault including kids, however it doesn't expressly include AI-generated content.[188] Norway is prepared to follow larger the European Union and Council of Europe rules, nevertheless, by means of programs like CIRCAMP.

Overall, Europe's national addresses to AI-generated CSAM are still not well coordinated. Nations such as the United Kingdom, Sweden, and the Netherlands had regulations that are rather broad and include manufactured visuals. However, Germany and Norway still utilize laws which were created for more conventional kinds of abuse. Not having harmonization makes it harder to implement the law and makes it harder for countries to work together to fight an international and increasingly sophisticated type of child sexually abuse.

c. Legislation and Approach in the United State

The legal approach of the United States toward child sexual abuse material (CSAM) is shaped by a fundamental tension between First Amendment protections and the need to safeguard children from exploitation. This tension becomes especially pronounced in cases involving synthetic or AI-generated CSAM, which may not involve real children but nonetheless replicate sexual abuse in disturbing, photorealistic ways.[189] The First Amendment's strong protection for freedom of expression constrains legislative efforts that attempt to criminalise fictional content unless it meets the constitutional definition of obscenity or involves actual harm.

[186] Bertheubert (n 167); IWF (n 169)
[187] INHOPE (n 158) 362; UNCRC 2021 (n 150) para 79.
[188] Lovdata (n 176)
[189] Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence (CUP 2020) https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/an-introduction-to-the-law-ethics-and-policy-of-artificial-intelligence/68594ED27FD460DC1D77821AE15D4C94 244.

The Supreme Court's decision in Ashcroft v. Free Speech Coalition is a key legal precedent. In that case, the Court struck down two parts of the 1996 Child Pornography Prevention Act (CPPA) that made it illegal to show pictures that "appear to be" kids doing sexual acts. The Court said that these rules were too broad and violated free expression since they made it illegal to show things that were neither vulgar or the consequence of real abuse.[190] The decision created a big hole in how the federal government regulates synthetic CSAM.[191] It made it impossible to make fictitious or computer-generated child pornography illegal unless it could be shown to be obscene under the Miller test.[192]

In response, Congress enacted the PROTECT Act of 2003[193], which sought to narrow the scope of liability while responding to the Court's constitutional concerns. Rather than criminalising the possession of all virtual CSAM, the PROTECT Act targeted individuals who "pander" or "solicit" such content in a way that suggests it involves actual minors. This performative standard allows prosecution based on context or representation, even if the material is synthetic, provided it creates the impression that real children are involved. However, the statute does not criminalise the mere creation or possession of AI-generated material unless it is tied to fraud or exploitative intent.[194]

Due to the limitations of federal law, enforcement agencies have struggled to address synthetic CSAM shared in closed networks or generated for private use. Reports by the National Center for Missing and Exploited Children (NCMEC) underscore that AI-generated CSAM is increasingly indistinguishable from real imagery, and its proliferation undermines both enforcement efforts and survivor identification workflows.[195] Despite this, no comprehensive federal legislation has been passed to regulate AI-generated CSAM directly.

---

[190] Child Pornography Prevention Act of 1996, Pub L No 104–208, div A, tit I, § 121(1), 110 Stat 3009 (codified at 18 USC § 2256(8)(B)) https://www.congress.gov/bill/104th-congress/senate-bill/1237/text/is
[191] *Ashcroft v Free Speech Coalition* (n 32)
[192] Department of Justice, 'Citizen's Guide to U.S. Federal Law on Child Pornography' (2024) https://www.justice.gov/criminal/criminal-ceos/citizens-guide-us-federal-law-child-pornography accessed 3 July 2025.
[193] PROTECT Act of 2003, Pub L No 108–21, 117 Stat 650 (codified in part at 18 USC §§ 2251–2260A) https://www.congress.gov/bill/108th-congress/senate-bill/151 accessed 3 July 2025.
[194] Cambridge Handbook (n 189) 246.
[195] NCMEC, 'Generative AI CSAM is CSAM' (2024) https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam accessed 3 July 2025.

In contrast to federal inaction, some U.S. states have begun developing their own legal responses. Most notably, California passed Assembly Bill 1831 in 2024, making it the first U.S. state to explicitly criminalise the creation, possession, and distribution of AI-generated CSAM. The bill defines such material as "a visual depiction that is, or appears to be, of a minor engaging in sexual conduct, where the depiction was generated by artificial intelligence or a similar technology".[196] This standard departs from the federal model by explicitly recognising the potential symbolic and anticipatory harm of synthetic imagery and framing the offence in terms of representational impact rather than the presence of actual child victims.

California's approach was motivated by growing concerns that synthetic abuse imagery is facilitating child sexual exploitation, normalising paedophilic fantasies, and complicating content moderation.[197] AB-1831 received bipartisan support and backing from law enforcement, child advocacy groups, and digital rights organisations. Its passage marked a significant normative shift by treating AI-generated CSAM as a legitimate subject of criminal law, even in the absence of real harm.[198] Moreover, the bill includes aggravated sentencing provisions when such content is distributed with the intent to arouse, harass, or terrorise others.[199]

Parallel to California's legislative reform, more than 50 state attorneys general signed a joint letter urging Congress to adopt federal legislation to regulate AI-generated CSAM. The letter warned that existing laws are insufficient to address the scale and speed of generative technology and called for explicit prohibitions at the federal level.[200] The attorneys general cited the difficulty of prosecuting cases under current statutes, especially when the material is hosted abroad or produced in states with no relevant laws.[201]

State-level programs are still constrained in what they can do. The Connecticut Office of Legislative Studies did a study of the government's laws in 2024 and found that just a few

[196] AB-1831 (n 35)
[197] Politico, 'California Goes After AI-Generated Child Sexual Abuse' (16 January 2024) https://www.politico.com/newsletters/california-playbook/2024/01/16/california-goes-after-ai-generated-child-sexual-abuse-00135707 accessed 3 July 2025.
[198] The Register, 'Attorneys General Call for Federal Law on AI CSAM' (6 September 2023) https://www.theregister.com/2023/09/06/ai_csam_national_law_call/ accessed 3 July 2025.
[199] AB-1831 (n 35)
[200] Attorneys General of the United States, *Letter to Congress Regarding the Regulation of AI-Generated Child Sexual Abuse Material* (5 September 2023) https://regmedia.co.uk/2023/09/05/handout_ag_letter_csam.pdf accessed 3 July 2025.
[201] The Register (n 198)

states, like New York and Virginia, have introduced or thought about laws dealing with AI-generated CSAM. Many jurisdictions still use antiquated laws that don't take into account the intricacies of synthetic content.[202] For example, prohibitions against animated or cartoon pornography generally don't fulfil the standard set in Ashcroft.[203]

Recent criminal cases show even further how far behind the law is when it comes to technology. In 2024, U.S. law enforcement detained a number of people for making AI-generated CSAM on sites such as Stable Diffusion and sharing it on social media or private forums.[204] In several cases, attorneys relied on fraud or obscenity charges owing to the lack of appropriate child protection legislation. A well-known case featured an authorized child a psychiatrist who utilized AI methods to make CSAM and was punished under federal kid pornography statutes because some of the photographs in the dataset were real.[205]

Criminal specialists have said that using child exploitation databases for teaching artificial intelligence makes it much harder to judge CSAM legally and morally. The Stanford Internet Observatory's 2023 report said which artificial intelligence algorithms developed upon CSAM photos might make violent material, which means which the problem is related to the feedback and the production.[206] The constitutional position of such models is still up in the air, and legal systems have not yet decided if education artificial intelligence alongside CSAM counts as control or distribution according to the present laws.

Participants are additionally worried which media administrators and websites won't know how to deal with manufactured CSAM lacking explicit federal rules.[207] A 2023 Cellebrite study

[202] Connecticut Office of Legislative Research, '2024-R-0167: Artificial Intelligence and Child Pornography Laws' (April 2024) https://www.cga.ct.gov/2024/rpt/pdf/2024-R-0167.pdf
[203] Enough Abuse Campaign, 'State Laws Criminalizing AI-generated or Computer-Edited CSAM' (2024) https://enoughabuse.org/get-vocal/laws-by-state/state-laws-criminalizing-ai-generated-or-computer-edited-child-sexual-abuse-material-csam/ accessed 3 July 20205.
[204] PCMag, 'Man Arrested for Creating AI Child Sexual Abuse Material Using Stable Diffusion' (2024) https://www.pcmag.com/news/man-arrested-for-creating-ai-child-sexual-abuse-material-using-stable-diffusion accessed 3 July 2025; The Verge, 'AI CSAM on Instagram Leads to Arrest' (21 May 2024) https://www.theverge.com accessed 3 July 2025.
[205] Law & Crime, 'Child Psychiatrist Sentenced After Using Artificial Intelligence to Make Child Pornography' (2024) https://lawandcrime.com accessed 3 July 2025.
[206] Stanford Internet Observatory, *ML Training Data and CSAM: Assessing the Legal and Ethical Risks of Training AI Models on Harmful Content* (23 December 2023) https://stacks.stanford.edu/file/kh752sm9123/ml_training_data_csam_report-2023-12-23.pdf 12.
[207] Cellebrite, 'AI and CSAM: A Look at Real Cases' (2023) https://cellebrite.com/en/ai-and-csam-a-look-at-real-cases/ accessed 3 July 2025.

found that digital proof of AI-generated exploitation is typically destroyed or hidden before police can get involved, making it harder to investigate across borders.
California has gained further traction at the policy level with legislative measure 1394, that's concerned with abuse of children on digital media algorithms and works with AB-1831 to hold platforms accountable (AB-1394 2024). The measure doesn't specifically deal with AI-generated images, but it is part of a larger trend to recognize how algorithms might make exploitation easier.

In comparative perspective, the U.S. approach remains fragmented. While European jurisdictions have emphasised dignity-based and precautionary frameworks that allow for the criminalisation of synthetic content, U.S. law continues to hinge on obscenity, fraud, or child involvement. AB-1831 represents an emerging willingness to deviate from this model and address symbolic harm more directly, echoing the approach taken in jurisdictions such as Sweden and the Netherlands.[208]

In conclusion, the way the law handles AI-generated CSAM in the US shows that there is a difference among national and state methods, and that expression is strongly protected by the Constitution. Even if Ashcroft v. Free Speech Association still sets the limitations on government authority, new laws in several states, especially California, show a way forward. The way AB-1831 recognizes the figurative and anticipation hazards of digital pictures might be a precedent for later years changes. It's not certain if the legislature is going to adopt this example, but the current hodgepodge of rules and workarounds used by prosecutors is not enough to deal with the problems that generative technologies cause in the area of sexual abuse of kids.

2. Legal Gaps and Challenges in Enforcement

Even while more people are aware of the ethical and upright dangers of AI-generated sexually assaulting kids' material, current laws and regulations at both the domestic and international levels are still having trouble keeping up with this new problem. The preceding sections had shown which certain places made good headway in broadening the meaning of CSAM or making manufactured content illegal. However, these efforts are still scattered and not enough.

[208] INHOPE (n 158) 322.

Also, that remains a considerable difference among which modern technology may accomplish as well as what the law provides about it. This renders it hard to carry out the legislation and make sure it stays the same. There are legitimate blind spots because of old concepts about harm and victims, slow implementation of worldwide instructions, and an overall failure to reassess the limitations of law enforcement in the context of recent digital threats.

The suggested Redefining of Directive 2011/93/EU is a good first step in clearing up some of the legal confusion over synthetic CSAM at the European level. The new draft clearly states that "realistic or synthetic representations" are included and gives an overall description of material about child sexual abuse that takes into account today's threats. It goes beyond the previous guideline by taking into consideration new types of digital content, such as changes, deepfakes, and content made by AI. By doing this, it gives a clearer normative foundation for making things illegal and makes member states' procedural duties stronger when it comes to helping victims, coordinating across borders, and reporting procedures.

But even this advanced project doesn't fill up all the gaps in the law. One of the most important problems is that EU regulations are being slowly and unevenly added to national criminal laws. EU law says that member states must make their own laws fit with the goals and content of directives. However, this process might take several years. This legislative delay is not just a bureaucratic hassle; it is a major regulatory failure in the context of generative technologies that are moving quickly. The danger may have changed through the moment an order is put into effect, making national systems always behind the times. In an issue as important and delicate as child protection, these kinds of delays can have big effects on both enforcement and the legal system's ability to set standards for prohibited behaviour.

Also, the requirement to turn instructions into national legislation does not inevitably mean that the laws would be the same in practice. Member states have a lot of freedom in how they carry out these duties, especially when it comes to law enforcement, which is still tightly linked to national autonomy. Because of this, the way that European-level laws make manufactured material illegal can frequently be very different from how they are used in each country. Some states have broader definitions that incorporate AI-generated images under current CSAM rules, while others only hold people responsible for situations where the children can be identified.

This freedom of choice results in a patchwork of rules and ways of enforcing them that makes the European legal environment less coherent. It also makes it harder for police from different countries to work together on criminal cases since it's harder to agree on what counts as a crime when the laws are different.

It is especially worrying when the criminal codes in different countries don't match up. Some nations, like Sweden and the Netherlands, have stated added requirements based on appearance or changed the language of their laws to cover representations that "appear to" show children. However, many other countries have not changed their rules at all to deal with synthetic material. The legal system still doesn't see the harm caused by AI-generated CSAM in places where criminal culpability still depends on the involvement of a real kid. This isn't only a case of legislative oversight; it's also a case of conceptual stagnation. Many criminal law systems are still based on a materialist view of damage, which says that physical injuries or identifiable victims are required criteria for punishment. Because of this, symbolic, anticipatory, or structural damages, including the cultural normalization of child sexualization or the re-traumatization of survivors whose likenesses are scraped and copied, are frequently not covered by criminal law.

The structure of supranational instruments makes this conceptual restriction much worse. The Lanzarote Convention and other similar treaties let countries not make virtual CSAM illegal if no real kid is involved. This may have been a reasonable compromise when it was written, but it now shows an antiquated vision of sexual exploitation that doesn't take into account the new problems that generative AI has created. Without wording that makes the clauses obligatory and requires them to be enforced, these permissive clauses make uncertainty a part of the system. They provide states legal justification for not doing anything while making it look like there are consistent safety standards across Europe.

In this case, the new EU AI Act is likewise a good example. It recognizes that children are vulnerable and makes high-risk AI systems responsible for following the rules, but it doesn't include any criminal or liability regulations that are particular to AI-generated CSAM. It also doesn't talk about the rising worry about "abuse-trained" models, which are AI systems that have been trained on real child abuse photographs and may make fake versions of such images. There is a big conceptual and regulatory blind spot when it comes to not regulating the input side of AI-generated CSAM. It makes us think about how developers and platforms are

involved, as many of them are still protected from being held responsible even when they help make damaging material.

On the other hand, the United States has made more progress at the state level, even if the First Amendment limits what the federal government may do. California's Assembly Bill 1831, which makes it a crime to make CSAM with AI regardless of whether real kids are involved, is a groundbreaking example of innovation at the state level. It shows that you comprehend injury in a way that goes beyond just hurting someone physically; it also involves expressive and cultural harm. But other states haven't followed California's path yet. Because of this, the U.S. terrain is full of jurisdictional discrepancies, which means that criminals can take advantage of variances in where they live to avoid punishment. This makes it harder Rendition less effective and makes India's prosecution more difficult, especially when content crosses Treasury or national boundaries.

The problem of enforcement is a bigger one that affects both the EU and the US. Even when synthetic CSAM is illegal, police generally don't have the technological resources or forensic skills to find, analyse, and tell the difference between this kind of material and true misuse. Diffusion models and generative adversarial networks generate information that seems very lifelike, which makes it hard to classify by hand. Automated detection algorithms have a hard time with situations that aren't clear, and the databases that are already out there are mostly for matching genuine images, not for finding new synthetic material. If there isn't a lot of money put into new forensic technologies and training, changes to the law might just be for show instead of being useful.

Another area that hasn't been looked at enough is the involvement of private players, especially digital platforms and AI developers. Companies don't have to do anything legally to find or stop the formation of fake CSAM on their platforms or with their tools right now. Some places have content moderation frameworks; however, they are typically not binding or only reactively. As AI tools grow more decentralized and easier to use, the likelihood of "DIY" CSAM creation rises, and so does the difficulty of figuring out who is to blame. To make sure that generative technologies are used safely, we need to reconsider who is responsible for them. This includes not only users but also the people who build, distribute, and make money from them. If you don't deal with these systemic facilitators, any reaction to crime will be inadequate and useless in the end.

Lastly, the fact that different countries are taking different approaches to the problem might make it harder to fight online child sexual exploitation on a larger scale. Cross-border investigations will continue to be difficult without a common legal norm or a clear definition of what synthetic CSAM is. Offenders will keep taking advantage of gaps in the law, and victims both actual and symbolic will not have enough legal protection. To make sure that generative AI is regulated in a way that is consistent, encourages collaboration in enforcement, and includes a child-rights-based point of view, we may need an international treaty, or a framework sponsored by the UN.

3. Conclusion

There are big holes in the rules around AI-generated CSAM which have been present over a long time and are still there when it comes to theoretical law, regulation, and working together with other countries. The Redefining Regulation and other tools have helped the EU become more consistent, but state execution is still delayed and varied, which makes global attempts less successful. Numerous puts still use old ideas about damage and victims in their statutes, which don't reflect the complex reality of manufactured assault on women. In the meantime, the US is a mixed bag, with new laws such as California's AB-1831 living with gaps in the law in other states.

Enforcement tools also can't keep up with how quickly technology changes, and there are still few rules around how private companies might help or enable synthetic CSAM. As generative technologies get stronger and easier to use, the hazards will only grow. To close these gaps, we need to change the way we think about damage, accountability, and the role of criminal law in the digital era, as well as make changes to the law. Without these kinds of measures, keeping kids safe online will always be partial, reactive, and not good enough.

CHAPTER V: SUGGESTED LEGAL FRAMEWORK

1. Conceptualising the Crime in AI-generated CSAM?

Three fundamental tenets have long served as the cornerstones of the legal conceptualisation of crime: the existence of a recognisable victim, evidence of harm, and the transgression of a well-defined legal standard. Each of these is methodically contested by AI-generated child sexual abuse material. AI-CSAM appears to elude traditional criminal law because there is no actual child physically present, no direct harm is proven, and legal standards are based on antiquated technological presumptions. However, the absence of living victim does not negate the existence of violence or wrongdoing. According to this thesis, in order to maintain moral and communicative purposes of criminal law, AI-generated CSAM needs to be viewed as a separate criminal category that represents representational abuse, symbolic harm, and anticipatory risk.

The classic three elements of criminal law actus reus, mens rea, and a tangible result often damage to an individual or legally protected interest are heavily weighted in conventional criminal law, particularly in liberal legal regimes.[209] Feinberg's original idea of the damage principle is that acts should only be made illegal if they hurt someone else's interests without a good reason. AI-CSAM is not a crime according to these criteria because it doesn't utilize real kids and usually doesn't hurt anyone. Feminist law enforcement, like Intelligent, possesses long pointed out that the law's focus on concrete evidence and personal damage sometimes misses systematic assault and oppression in general.[210]

Decentring physicality as the main site of harm is the first step towards conceptualising AI-CSAM as a crime. Even though the image is artificial, it is still a performative act. It creates meaning, arouses desire, and infiltrates digital cultures with narratives of exploitation. Here, Ronald C. Kramer's concept of "wilful social harm" is particularly helpful. Even in the absence of a specific victim, Kramer contends that certain actions compromise institutional integrity and social values.[211] AI-CSAM challenges the widely held moral belief that children should not be sexualised, commodified, or treated as objects of adult fantasy by simulating abuse. This

[209] Feinberg (n 62)
[210] Carol Smart *Feminism and the Power of Law* (Routledge 1989) 130.
[211] Kramer (n 81) 4.

is a public wrong not because a child is harmed directly, but because the symbolic framework of protection is broken.

Such a rethinking is further justified by the communicative role of criminal law. According to Duff, criminal law should convey the community's disapproval of actions that jeopardise its normative commitments, rather than merely serving as a deterrent or a means of punishment.[212] The crime of AI-CSAM lies not in its capacity to injure a specific child, but in its ability to blur the line between childhood and sexual availability. Even when completely fictional, the creation and distribution of such material conveys the message that child sexualisation is acceptable. Thus, AI-CSAM constitutes what Feinberg calls an "expressive wrong" -a violation that is wrongful because of the message it communicates, not necessarily the harm it causes.[213]

The representational aspect of violence has also been underscored by feminist scholars. Carol Smart critiques the legal system for failing to account for how women and girls are framed as passive objects in both cultural and legal narratives. AI-CSAM contributes to precisely this architecture. It constructs and distributes digital representations of childhood sexuality, often based on gendered stereotypes that render young girl's consumable. Even though the images are artificial, they reinforce patriarchal norms and feed a broader ecosystem of age-based subordination and misogyny. AI-CSAM, therefore, is not victimless. Its structural victims include the social meaning of innocence, the symbolic figure of the child, and the very concept of protection that child safeguarding laws claim to uphold.[214]

According to this revised paradigm, the criminality of AI-CSAM is not contingent upon the realism of the image or the presence of a real child. Instead, its foundations lie in three interrelated dimensions: (1) the damage it does to the public moral order via expressive content; (2) the harm inflicted upon categories of personhood, such as childhood and girlhood; and (3) the risk of desensitisation and normalisation of deviant desire. Even in the absence of a named victim, these factors produce a "compound harm" that justifies criminal intervention.

Accordingly, the definition of crime must evolve. AI-CSAM should be considered a "representational crime" or "symbolic crime" -one that violates shared moral codes, even if no

[212] Duff (n 70) 80.
[213] Feinberg, *Offense to Others* (Oxford University Press 1985) 38.
[214] Carol Smart, *Women, Crime and Criminology: A Feminist Critique* (Routledge 1976) 32.

direct physical consequence occurs. This logic already underpins laws on hate speech, Holocaust denial, and racist propaganda, which criminalise expression not because of injury but because of its corruptive social power. AI-CSAM similarly constitutes a form of symbolic domination and moral transgression that warrants legal response.

Also, this new way of seeing things fits with the ideas of preventative fairness. The author says that certain behaviours should be criminalized rather than since they have caused damage, however since the danger and figurative breach are too high to overlook. AI-CSAM is being utilized more and more in online forums, role-playing settings, and cleaning, where it makes interaction offenses more likely.[215] The Internet Watch Foundation has said that this kind of content is no longer just made up; it is part of genuine deviant behaviours and societies associated with electronic abuse.[216] So, making AI-CSAM illegal serves as a way to stop it and also a way to voice yourself.

In short, AI-generated CSAM makes us rethink what this means to be an offender in the age of the internet. It shows how harm-based and victim-centred ideas don't always work and stresses legislation's eloquent figurative, and preventative roles. Recognizing AI-CSAM as a figurative crime permits the judiciary to do its job of protecting democratic principles and respect, not only punishing people.

2. Reconstructing Victimhood in AI-generated CSAM

The concept of victimhood is fundamental to criminal law, which traditionally requires a tangible harm inflicted upon an identifiable individual. In cases involving AI-generated child sexual abuse material (AI-CSAM), this framework is disrupted, as such content can be created without the use of any real child. Consequently, some scholars have referred to AI-CSAM as a "victimless crime," arguing that the absence of a directly harmed person precludes criminal liability. This section challenges that assumption and reconsiders victimhood through alternative conceptual lenses -symbolic, structural, and collective- to argue that AI-CSAM does, in fact, create victims, albeit in more complex and dispersed ways.

[215] Andrew Ashworth and Lucia Zedner, *Preventive Justice* (Oxford University Press 2013) 89.
[216] Internet Watch Foundation, *AI-generated Child Sexual Abuse Material: Threat Assessment Report* (2024) https://www.iwf.org.uk accessed 3 July 2025.

According to Feinberg, injury is "the wrongful setback of interests." The idea of victimization depends on the impairment of a legitimate interest.[217] The legal system's long-standing focus on direct, physical suffering ignores other types of harm, especially those that include symbolic enslavement. Feminist legal theorists have been saying for a long time that the law doesn't take into consideration how gendered power works via symbolic forms of control. For example, Smart says that legal discourse doesn't pay enough attention to how women and girls are always seen as docile, obedient, and accessible.[218] AI-generated CSAM copies and intensifies this kind of representational violence by showing children, especially girls, in sexually explicit and demeaning situations. This reinforces societal scripts that sexualize and objectify children.

Chesney-Lind and Pasko call this kind of damage "fundamental victimization," that means that it doesn't just happen on a personal level, however, is also built into social conventions and constitutional gaps.[219] AI-CSAM breaks down the line between kids as people and kids as sexual objects, which is a symbolic way of taking away childhood. Even if there isn't an actual child, this kind of content hurts our shared ideas about youth and weakens the safeguards that society gives to kids.

Also, AI-CSAM is occasionally separate from genuine victims. Thiel and his team found that numerous machine learning algorithms were developed on genuine CSAM databases. This means that the pain of real children is built into the machine's logic and might be duplicated in synthetic outputs. In these situations, the idea of revictimization becomes real: children are hurt again by the spread of derivative content, even though the outputs don't seem like them anymore. The Internet Watch Foundation also says that photographs of kids that are disseminated openly, frequently on social media, are being used to make deepfake CSAM, which combines genuine faces with fake bodies.[220]

We may also look at victimization on a group level. R.A. Duff says that criminal law does more than only punish people; it also shows that people in a political environment possess ethical censure and strengthens their beliefs.[221] Even if it doesn't include an actual youngster, the spread of AI-CSAM goes against what society expects from people who want to keep kids safe.

---

[217] Feinberg (n 62) 34.
[218] Smart (n 214) 87.
[219] Chesney-Lind and Pasko (n 104) 21.
[220] CameraForensics, 'A Guide to AI-generated CSAM for Investigators of Online Exploitation' (2024) https://www.cameraforensics.com/blog/2024/11/18/a-guide-to-ai-generated-csam-for-investigators-of-online-exploitation/ accessed 3 July 2025.
[221] Duff (n 70) 90.

Kramer has said that these kinds of actions are "wilful social harm" because they hurt society's values and weaken the rules that keep communities secure.[222]

This broader view of harm is not unprecedented. Legal systems already recognize offenses without individualized victims -such as hate speech or incitement to violence- on the basis that they endanger public values. Similarly, AI-CSAM may be punished not only because it harms a specific person, but because it threatens the normative order that protects vulnerable populations.

In sum, the question “who is the victim?” in the context of AI-generated CSAM cannot be answered through a narrow lens. Victimhood must be reconstructed in pluralistic terms: it may be personal (when images are generated using identifiable features or training data), representational (when cultural conceptions of childhood are degraded), or communal (when the safety of the moral community is compromised). Recognizing these forms of harm does not weaken the argument for criminalization -it strengthens it by aligning the law with the evolving realities of digital violence. In AI-CSAM, the victim is not absent; they are dispersed across layers of code, culture, and shared vulnerability.

4. Developers’ Liability

The rise of productive artificial intelligence (AI) has made it possible for more people to be involved in making material related to child sexual abuse. In the past, end-users those who acquire, generate, or share illegal content have been the ones most responsible for crimes. But when it comes to AI-generated CSAM, especially photorealistic or deepfake images, it's reasonable to say that the creators and producers of the AI systems that make this possible are also responsible. This part says that developers here, not person programmers but firms and organizations that create and implement large-scale artificial intelligence systems have a constitutional and ethical obligation to think ahead and do all they can to reduce the dangers which come from individuals using its innovations in manners which are not intended.

AI-generated material is different from traditional CSAM since it doesn't need an actual child to be involved. Instead, it may be made using general-purpose artificial intelligence models trained on enormous datasets that aren't always well-filtered. Stability, Midjourney, and open-source versions of LLaMA are among of the models that have been quite useful for making

[222] Kramer (n 81) 8.

very realistic exploitation modelling. Studies have shown that a number of these algorithms were developed on datasets taken from the web without enough small amounts, which means that sexualized or improper pictures of kids have been included in the training data.[223] While builders make these kinds of technologies available to others lacking good protections, they not only make it easier for digital damage to happen, but they also help it happen.

OpenDream is a scary example. It was an AI picture production platform that advertised its capabilities as an art instrument but also let people make AI-generated CSAM. Bellingcat along with other investigators found that OpenDream users often made and shared fake child abuse material, at times including instructions that described made-up adolescents' individuals, anime-style children, and sometimes real children's names. Even though people in the community complained and there was obvious proof of exploitation, the platform didn't have good moderation measures and kept running until lenders stepped in.[224] This scenario shows what may happen when builders or vendors of platforms don't do even the smallest things to stop people from using their products in ways that are easy to anticipate coming.

These kinds of situations make us think about important legal problems concerning how much developers are responsible. The 230th chapter of the Act on Communication Decency gives platforms a lot of protection from user-generated material in the United States.[225] But this protection does not cover developers or suppliers that intentionally help or promote the creation of illicit material. Section 230 was not created with artificial intelligence in mind either. As experts have pointed out, the law's old ideas about passive hosting don't work well with the engaged, content-producing characteristics of models created by AI.[226]

Similarly, while the PROTECT Act[227] criminalises certain types of virtual child pornography, including "pandering" and "soliciting" behaviour that gives the impression of involving real minors, it remains silent on the responsibilities of those who develop or distribute AI systems used to generate such imagery. This legal silence allows developers to evade liability by

[223] Thiel et al. (n 117) 9.
[224] Kolina Koltai, 'OpenDream: Secretive AI Platform Broke Stripe Rules to Rake in Money from Nonconsensual Pornographic Deepfakes' (Bellingcat, 14 October 2024) https://www.bellingcat.com/news/2024/10/14/opendream-ai-image-generation-csam-vietnam accessed 3 July
[225] Communications Decency Act, 47 USC § 230 (1996).
[226] Meg Hennessey, 'AI-Generated Child Sexual Abuse Material: How Companies Can Reduce Risk' (Orrick, 2024) https://www.orrick.com/en/Insights/2024/02/AI-Generated-Child-Sexual-Abuse-Material-How-Companies-Can-Reduce-Risk accessed 3 July 2025.
[227] PROTECT Act (n 193)

distancing themselves from the content their systems generate -often claiming neutrality or lack of intent.

But this argument gets weaker and worse when developers offer foundation models with established risk profiles. Child protection specialists and scholars are worried about the open-source dissemination of strong diffusion models. corporations Magazine: "When companies release systems without quick filtering, watermarking, or content moderation tools, they are basically asking for trouble." When such systems are also trained on datasets that may have abusive content or stolen pictures of kids, it's hard to believe that they don't know what they're doing.[228]

This is where the idea of "anticipatory responsibility" becomes very important. Ashworth's theory of preventative justice says that culpability can come from more than simply causing harm; it can also come from making situations more dangerous. This framework includes developers that make AI tools that can make fake CSAM available to the public without any filters. Not including fundamental guardrails, monitoring outputs, or limiting specific usage are all examples of structural carelessness.[229]

Feminist legal theory gives a different kind of criticism. According to Carol Intelligent, judicial structures frequently don't take into account the way fundamental and figurative damages are built into the design of technology and societal contexts. In this case, builders are not just engineers; they are also the people who design platforms that make sexualizing minors acceptable, strengthen abusive strength of authority, and repackaging exploitation as imaginative thinking.[230] Programmers who don't think about these effects, or more severe, put free markets ahead of moral protection, are part of the framework that fosters electronic aggression.

European regulatory frameworks have begun to reflect this shift. The AI Act of the European Union, particularly its provisions on general-purpose AI (GPAI), imposes transparency, risk assessment, and documentation obligations on model providers. Although not yet in full effect, the Act suggests that companies deploying powerful models must account for potential misuse, including the generation of illegal content like CSAM. The GPAI Belgrade Declaration further

[228] Internet Watch Foundation, 'AI-Generated CSAM: Threat Assessment' (IWF 2024) https://admin.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf accessed 3 July 2025
[229] Ashworth and Zedner (n 215)
[230] Smart (n 214) 62.

reinforces this approach by calling on developers to adopt safety-by-design practices and implement anticipatory due diligence when building or releasing AI systems.[231]

However, EU regulatory instruments also face implementation delays. The Digital Services Act requires large online platforms to monitor and mitigate illegal content but remains ambiguous on its application to AI models themselves. In practice, this means that developers may escape liability if they release foundation models but do not operate platforms directly hosting generated outputs. California's Assembly Bill 1831 represents a more robust intervention, explicitly criminalising the production of AI-generated CSAM and allowing for penalties against those who "produce or facilitate" the means of such production. Though not yet tested in court, the bill suggests a path forward for future legislation targeting developers.[232]

Ultimately, the legal system must move beyond outdated dichotomies that separate tool from use, intent from outcome, or developer from user. In the realm of AI-generated CSAM, the risks are not hypothetical, they are documented, foreseeable, and actively exploited. Developers, especially corporate entities releasing GPAI systems into public hands, must bear responsibility not only for what their systems are designed to do, but also for what they are capable of doing when placed in unregulated environments. Criminal law, as well as civil liability frameworks, must evolve to reflect this new technological reality.

5. Conclusion

This chapter has proposed a normative redefinition of crime, victimhood, and liability in the context of AI-generated child sexual abuse material. It argued that existing legal paradigms - rooted in physical harm, real victims, and narrow constructs of culpability- are insufficient to address the representational, symbolic, and anticipatory harms produced by synthetic CSAM. By reconceptualising AI-CSAM as a "symbolic crime," and acknowledging its impact on public morality, childhood dignity, and cultural narratives of sexualisation, this framework justifies its criminalisation not despite the absence of a real child, but because of its corrosive social meaning. The chapter also reaffirmed that victimhood could exist beyond the material body, affecting individuals through digital proximity, identity misappropriation, and cultural degradation

[231] Global Partnership on AI (GPAI), *Belgrade Declaration* (2024a) https://wp.oecd.ai/app/uploads/2024/12/GPAI-Belgrade-Declaration-final-3.pdf accessed 3 July 2025.
[232] AB 1831 (n 35)

Equally crucial is the shift in responsibility from mere users to upstream actors such as developers and platform providers. The capacity of AI systems to industrialise abuse without oversight creates an urgent need for anticipatory regulation and legal accountability. Developers must be held to higher standards of risk mitigation, transparency, and ethical design. Moving forward, criminal law must not only adapt to technological change but also expand its moral and protective mandate to defend vulnerable categories, such as childhood, not only as bodies, but as social values.

CHAPTER VI: GENERAL CONCLUSION

This thesis has argued that AI-generated child sexual abuse material (AI-CSAM) ought to be criminalised, even in the absence of a real, identifiable child, due to the symbolic, structural, and anticipatory harms it generates. Traditional criminal law frameworks -rooted in tangible harm and individual victimhood- are no longer sufficient in the face of rapidly evolving generative technologies. AI-CSAM poses a unique threat not because it directly violates bodily integrity, but because it undermines the moral and legal category of childhood itself. It weakens the social boundaries that separate innocence from exploitation, and in doing so, inflicts a profound form of symbolic violence that legal systems can no longer afford to ignore.

Central to this argument is the principle of the best interests of the child, a cornerstone of international human rights law. This principle must be prioritised above technological convenience, developer immunity, or formalistic interpretations of harm. The law should not only respond reactively to injury but should function proactively anticipating and preventing foreseeable harm. As demonstrated in frameworks such as the Istanbul Convention, prevention is not merely aspirational, but a legal obligation. To permit the production and circulation of AI-CSAM on the grounds that "no real child was harmed" is not a legal necessity, but a political choice, one that tacitly permits the symbolic violation of children.

Moreover, this thesis has highlighted the urgency with which criminal law must evolve to meet the challenges of emerging technologies. States have been swift to regulate digital markets, intellectual property, and cybersecurity in defence of economic or strategic interests. Yet, when it comes to the protection of children's dignity and integrity, legal responses remain fragmented, delayed, and often inadequate. This discrepancy must be addressed. Law is not merely a mechanism for punishment -it is a normative tool that defines the boundaries of acceptable behaviour, shaping the moral architecture of society.

For criminal law to fulfil this role, both its doctrinal structure and normative orientation must adapt. A reconceptualisation is necessary -one that acknowledges symbolic, structural, and anticipatory forms of harm as legitimate grounds for criminalisation. This demands a child-centred and feminist perspective that considers the dynamics of power, representation, and systemic vulnerability. Legal systems must go beyond physical harm and recognise that digitally mediated abuses, such as AI-generated CSAM, can reproduce and even intensify

patterns of subordination and exploitation. While such content may not involve physical contact, it degrades, distorts, and commodifies the image of the child, contributing to the normalisation of abuse and the erosion of protective norms.

In conclusion, the criminalisation of AI-generated CSAM is not an expansion of punitive power -it is a reaffirmation of criminal law's expressive, protective, and preventive functions. If the law is to remain a meaningful guardian of children's rights in the digital age, it must respond to new forms of violence with clarity and conviction. A failure to do so risks rendering the law morally hollow and normatively irrelevant in the face of evolving threats.

BIBLIOGRAPHY

Articles

Al-Alosi H, *The Criminalisation of Fantasy Material: Law and Sexually Explicit Representations of Fictional Children* (Routledge 2018) https://lccn.loc.gov/2018001996

Bentham J and Bennett J, *An Introduction to the Principles of Morals and Legislation* (2017) https://www.earlymoderntexts.com/assets/pdfs/bentham1780.pdf

Brown R, 'Property Ownership and the Legal Personhood of Artificial Intelligence' (2021) 30(2) *Information & Communications Technology Law* 21-22 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746768

Cassell PG and Morris MR Jr, 'Defining "Victim" through Harm: Crime Victim Status in the Crime Victims' Rights Act and Other Victims' Rights Enactments' (2024) *Utah Law Faculty Scholarship* https://dc.law.utah.edu/scholarship/392/

Cetinic E and She J, 'Understanding and Creating Art with AI: Review and Outlook' (2021) *arXiv.org* https://arxiv.org/abs/2102.09109

Chadha A, Kumar V, Kashyap S and Gupta M, 'Deepfake: An Overview' in *Lecture Notes in Networks and Systems* (2021) 557-566 https://doi.org/10.1007/978-981-16-0733-2_39

Chambers C, 'Reasonable Disagreement and the Neutralist Dilemma: Abortion and Circumcision in Matthew Kramer's Liberalism with Excellence' (2020) *New Genetics and Society* https://doi.org/10.17863/CAM.25317

DeLago C and others, 'Children Who Engaged in Interpersonal Problematic Sexual Behaviors' (2019) 105 *Child Abuse & Neglect* 104260 https://doi.org/10.1016/j.chiabu.2019.104260

Duff RA, *Answering for Crime* (2006) 106 *Proceedings of the Aristotelian Society* 87 https://doi.org/10.1111/j.1467-9264.2006.00140.x

Epstein Z, Hertzmann A and Investigators of Human Creativity, 'Art and the Science of Generative AI' (2021) *journal-article* https://ide.mit.edu/wp-content/uploads/2023/07/science.adh4451-1.pdf

Henry N, Flynn A and Powell A, 'Image-Based Sexual Abuse: Victims and Perpetrators' (2019) *Australian Institute of Criminology* 572 https://www.aic.gov.au/sites/default/files/2020-05/imagebased_sexual_abuse_victims_and_perpetrators.pdf

Insoll T and others, 'Risk Factors for Child Sexual Abuse Material Users Contacting Children Online' (2022) *Journal of Online Trust and Safety* https://doi.org/10.54501/jots.v1i2.29

Jurasz O and Barker K, 'Sexual Violence in the Digital Age: A Criminal Law Conundrum?' (2021) http://oro.open.ac.uk/78691/1/Jurasz%20Barker_Sexual%20violence%20in%20the%20digital%20age%20a%20criminal%20law%20conundrum%20%282021%29.pdf

Kleinfeld J, 'A Theory of Criminal Victimization' (2013) 65 *Stanford Law Review* 1087 https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2013/06/Kleinfeld_65_Stan._L._Rev._1087.pdf

Kokolaki E, Fragopoulou P and Foundation for Research and Technology - Hellas (FORTH), Institute of Computer Science, 'Unveiling AI's Threats to Child Protection: Regulatory Efforts to Criminalize AI Generated CSAM and Emerging Children's Rights Violations' (2024) *SafeLine* 1 https://arxiv.org/pdf/2503.00433

Koos S, 'A Normative Framework for Artificial Intelligence: Between Legal Subjectivity and Regulatory Instrumentalism' (2023) 5(1) *Technology and Regulation* https://doi.org/10.33102/mjsl.vol6no3.135

Kolen E, 'A Modern Tale of Frankenstein?: How to Regulate Non-Consensual Sexually Explicit AI-Generated Deepfakes in the Metaverse' (2024)

Kramer RC, 'Defining the Concept of Crime: A Humanistic Perspective' (1985) 12 *The Journal of Sociology & Social Welfare* 2 https://doi.org/10.15453/0191-5096.1715

Marshall B, 'No Legal Personhood for AI' (2023) 4 *Patterns* 100861 https://doi.org/10.1016/j.patter.2023.100861

McGlynn C and others, "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse" (2020) 30 Social & Legal Studies 541 https://doi.org/10.1177/0964663920947791

Okolie C, 'Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns' (2023) 25 *Journal of Internet Law* https://vc.bridgew.edu/cgi/viewcontent.cgi?article=3079&context=jiws

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

Pfefferkorn R, 'Addressing Computer-Generated CSAM: A Normative and Legal Framework' (2024) https://s3.documentcloud.org/documents/24403088/adressing-cg-csam-pfefferkorn-1.pdf

Salter M and Wong T, 'Parental Production of Child Sexual Abuse Material: A Critical Review' (2023) 25 *Trauma Violence & Abuse* 1826 https://doi.org/10.1177/15248380231195891

Stratton J and Powell A, 'Crime and Justice in Digital Society: Towards a "Digital Criminology"?' (2021) 17 *International Journal for Crime, Justice and Social Democracy* 5 https://www.crimejusticejournal.com/article/view/865

Trivison A, 'Understanding the Line between Art and Abuse: How Generative AI Changes the Landscape of Child Sexual Abuse Materials' (2024) 33 *Journal of Law and Technology* https://scholarship.law.edu/jlt/vol33/iss1/6

Witting SK, 'Child Sexual Abuse in the Digital Era: Rethinking Legal Frameworks and Transnational Law Enforcement Collaboration' (2020) https://hdl.handle.net/1887/96242

Yang Z, Zhan F, Liu K, Xu M and Lu S, 'AI-Generated Images as Data Source: The Dawn of Synthetic Era' (2023) *arXiv.org* https://arxiv.org/abs/2310.01830

Yu X and others, 'Fake Artificial Intelligence Generated Contents (FAIGC): A Survey of Theories, Detection Methods, and Opportunities' (2024) *arXiv.org* https://arxiv.org/abs/2405.00711

Books

Braithwaite J, *Restorative Justice and Responsive Regulation* (Oxford University Press 2001)

Brudner A, *Punishment and Freedom* (Oxford University Press 2009)

Chesney-Lind M and Pasko L, *The Female Offender: Girls, Women, and Crime* (2013)

Doak J, 'Defining Victim Through Harm: Crime Victim Status in the Criminal Process' in Matthew Hall, Joanna Shapland and Julian V Roberts (eds), *Victims of Crime: Problems, Policies and Programs* (2nd edn, Palgrave Macmillan 2021)

Feinberg J, *Harm to Self: The Moral Limits of the Criminal Law* (Oxford University Press 1984)

Feinberg J, 'The Classic Debate' in *Philosophy of Law* (Boston, MA: Cengage Learning, 2004)

Feinberg J, 'The Expressive Function of Punishment' (1965)

Fingarette H, 'Punishment and Suffering' (1977) 50 *Proceedings and Addresses of the American Philosophical Association* 499

Fletcher GP, *The Grammar of Criminal Law: American, Comparative, and International Volume One: Foundations* (Oxford University Press 2007)

Fletcher GP, 'The Place of Victims in the Theory of Retribution' (1999) 3 *Buff Crim L Rev* 51

Hampton J, 'The Moral Education Theory of Punishment' (1984) 13 *Philosophy & Public Affairs* 208

Husak D, *Overcriminalization: The Limits of the Criminal Law* (Oxford University Press 2008)

Kokolaki V, 'Digital Harm and Victimhood in the Context of AI-Simulated Abuse' in *Sexual Violence in the Digital Age* (Springer 2021)

Moore M, 'The Moral Worth of Retribution' in *Oxford University Press eBooks* (2010) https://doi.org/10.1093/acprof:oso/9780199599493.003.0003

Ring S, Gleeson K and Stevenson K, *Child Sexual Abuse Reported by Adult Survivors* (Routledge 2022)

Smart C, *Women, Crime and Criminology: A Feminist Critique* (Routledge 1976)

Zehr H, *Changing Lenses: A New Focus for Crime and Justice* (Herald Press 1995)

Zehr H and Gohar A, *The Little Book of Restorative Justice* (Good Books 2003)

Online Sources

Bellingcat, Kolina Koltai, 'OpenDream: Secretive AI Platform Broke Stripe Rules to Rake in Money from Nonconsensual Pornographic Deepfakes' (Bellingcat, 14 October 2024) https://www.bellingcat.com/news/2024/10/14/opendream-ai-image-generation-csam-vietnam accessed 3 July 2025.

CameraForensics, 'A Guide to AI-generated CSAM for Investigators of Online Exploitation' (2024) https://www.cameraforensics.com/blog/2024/11/18/a-guide-to-ai-generated-csam-for-investigators-of-online-exploitation/ accessed 3 July 2025.

Cellebrite, 'AI and CSAM: A Look at Real Cases' (2023) https://cellebrite.com/en/ai-and-csam-a-look-at-real-cases/ accessed 3 July 2025.

Cordeiro V C, "Combating the Rise of AI-Generated Child Sexual Abuse Material" (2025) https://www.humanium.org/en/combating-the-rise-of-ai-generated-child-sexual-abuse-material/.

EFF, Hayley Tsukayama, India McKinney, and Jamie Williams, 'Congress should not rush to regulate deepfakes' (Electronic Frontier Foundation, 26 June 2019) https://www.eff.org/deeplinks/2019/06/congress-should-not-rush-regulate-deepfakes.

Enough Abuse Campaign, 'State Laws Criminalizing AI-generated or Computer-Edited CSAM' (2024) https://enoughabuse.org/get-vocal/laws-by-state/state-laws-criminalizing-ai-generated-or-computer-edited-child-sexual-abuse-material-csam/ accessed 3 July 2025.

INHOPE, 'How the Recast EU CSAM Directive Empowers INHOPE Hotlines' (INHOPE, 2024) https://inhope.org/EN/articles/how-the-recast-eu-csam-directive-empowers-inhope-hotlines accessed 3 July 2025.

Korte L and Gardiner D, 'California Goes After AI-Generated Child Sexual Abuse' (Politico, 16 January 2024) https://www.politico.com/newsletters/california-playbook/2024/01/16/california-goes-after-ai-generated-child-sexual-abuse-00135707 accessed 3 July 2025.

NCMEC, 'Generative AI CSAM is CSAM' (2024) https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam accessed 3 July 2025.

Nudify Blog, 'A Step-by-Step Guide to Nudifying Photos' https://www.nudify.me/blog/a-step-by-step-guide-to-nudifying-photos accessed 30 June 2025.

PCMag, 'Man Arrested for Creating AI Child Sexual Abuse Material Using Stable Diffusion' (2024) https://www.pcmag.com/news/man-arrested-for-creating-ai-child-sexual-abuse-material-using-stable-diffusion.

Quach K, 'Attorneys General Call for Federal Law on AI CSAM' (The Register, 6 September 2023) https://www.theregister.com/2023/09/06/ai_csam_national_law_call/ accessed 3 July 2025.

Struckman K, 'Combatting AI-Generated CSAM' (Wilson Center, 27 November 2023) https://www.wilsoncenter.org/article/combatting-ai-generated-csam accessed 2 July 2025

Thorn, ‘What is CSAM? Child Safety Terms & Definitions’ (2025) https://safer.io/resources/common-terms-and-definitions/.

Tsukayama H, McKinney I and Williams J, ‘Congress should not rush to regulate deepfakes’ (EFF, 26 June 2019) https://www.eff.org/deeplinks/2019/06/congress-should-not-rush-regulate-deepfakes.

Van den Bergh C, ‘AI’s Chilling Impact on Child Sexual Abuse Material: A Wake-up Call for the International Community’ (Global Campus of Human Rights) https://www.gchumanrights.org/preparedness/ais-chilling-impact-on-child-sexual-abuse-material-a-wake-up-call-for-the-international-community/ accessed 2 July 2025.

Verge, ‘AI CSAM on Instagram Leads to Arrest’ (21 May 2024) https://www.pcmag.com/news/man-arrested-for-creating-ai-child-sexual-abuse-material-using-stable-diffusion accessed 3 July 2025.

Wired, ‘Sweden Sour on Kid Porn’ (1 May 1998) https://www.wired.com/1998/05/sweden-sour-on-kid-porn/ accessed 6 July 2025.

‘What Is Child Sexual Abuse Material?’ https://www.inhope.org/EN/articles/child-sexual-abuse-material

Other Sources

Attorneys General of the United States, *Letter to Congress Regarding the Regulation of AI-Generated Child Sexual Abuse Material* (5 September 2023) https://regmedia.co.uk/2023/09/05/handout_ag_letter_csam.pdf

Bert Hubert, 'Dutch Intelligence Service (AIVD) on CSAM: Update and Concerns' (2024) https://berthub.eu/articles/posts/dutch-intel-service-csam-update/ accessed 3 July 2025.

Connecticut Office of Legislative Research, '2024-R-0167: Artificial Intelligence and Child Pornography Laws' (April 2024) https://www.cga.ct.gov/2024/rpt/pdf/2024-R-0167.pdf

"Fight against Child Sexual Abuse: Updated Rules to Address New Technologies | News | European Parliament" https://www.europarl.europa.eu/news/en/press-room/20250613IPR28905/fight-against-child-sexual-abuse-updated-rules-to-address-new-technologies

United Nations, *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*, vols 2171–2171 (2000) https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/crc-sale.pdf

US Department of Justice and National Center for Missing & Exploited Children (NCMEC), *Child Sexual Abuse Material: Federal Response and Strategic Recommendations* (2023) https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf accessed 30 June 2025.

Reports

Bracket Foundation, 'Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse' (2024) https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf accessed 10 July 2025.

Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence (CUP 2020) https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/an-introduction-to-the-law-ethics-and-policy-of-artificial-intelligence/68594ED27FD460DC1D77821AE15D4C94

David Thiel, Leah Stroebel and Rebecca Portnoff, 'Identifying and Eliminating CSAM in Generative ML Training Data and Models' (Stanford Internet Observatory, 23 December 2023) https://stacks.stanford.edu/file/kh752sm9123/ml_training_data_csam_report-2023-12-23.pdf

INHOPE, 'Global CSAM Legislative Overview' (Second, 2024) https://inhope.org/media/site/e3bb326ed7-1729001643/global-csam-legislative-overview-2024-full-report.pdf accessed 3 July 2025.

Internet Watch Foundation, 'AI-Generated CSAM: Threat Assessment' (IWF 2024) https://admin.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf accessed 3 July 2025.

Internet Watch Foundation, 'AI-generated Child Sexual Abuse Material: Threat Assessment Report' (2024) https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/ accessed 5 July 2025.

Internet Watch Foundation (IWF), 'AI-Generated CSAM Report' (2023) https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

Internet Watch Foundation, 'The Online Safety Act (OSA) Explained' (IWF, 2024) https://www.iwf.org.uk/policy-work/the-online-safety-act-osa-explained accessed 3 July 2025.

Law Commission, 'Modernising Communications Offences: A Final Report' (Law Com No 399, 21 July 2021) https://assets.publishing.service.gov.uk/media/61ba022ad3bf7f05539de6f5/Modernising-Communications-Offences-2021-Law-Com-No-399.pdf

Sentencing Council, 'Response to Consultation: Sexual Offences Guidelines' (Sentencing Council, 2022) https://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Response_to_Consultation_web1.pdf accessed 3 July 2025.

Stanford Internet Observatory, 'ML Training Data and CSAM: Assessing the Legal and Ethical Risks of Training AI Models on Harmful Content' (23 December 2023) https://stacks.stanford.edu/file/kh752sm9123/ml_training_data_csam_report-2023-12-23.pdf

Legislation

Belgrade Declaration, Global Partnership on AI (2024) https://wp.oecd.ai/app/uploads/2024/12/GPAI-Belgrade-Declaration-final-3.pdf

Bill Text - AB-1831 Crimes: Child Pornography (California, 2023) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1831

Charter of Fundamental Rights of the European Union (2000) https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Child Pornography Prevention Act of 1996, Pub L No 104–208, div A, tit I, § 121(1), 110 Stat 3009 (codified at 18 USC § 2256(8)(B)).

Communications Decency Act, 47 USC § 230 (1996).

Convention on Cybercrime (Budapest Convention) (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185 https://rm.coe.int/1680081561

Coroners and Justice Act 2009 (UK) https://www.legislation.gov.uk/ukpga/2009/25/contents.

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) (adopted 25 October 2007, entered into force 1 July 2010) CETS No 201 https://rm.coe.int/1680084822

Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography [2011] OJ L335 https://eur-lex.europa.eu/eli/dir/2011/93/oj/eng.

Dutch Criminal Code (Wetboek van Strafrecht), art 240b https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Netherlands-Criminal-Code.pdf

European Parliament, Council of the European Union, and European Commission, "CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION" (2000) https://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Parliamentary Research Service, Criminalisation of Gender-Based Violence against Women: State of play and legislative developments in view of the Istanbul Convention and the proposed EU Directive on violence against women and domestic violence (Briefing, PE 762.374, June 2024) https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762374

General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1 https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

INHOPE, 'Recital 28 | EU Artificial Intelligence Act' https://artificialintelligenceact.eu/recital/28/

Law Commission, Modernising Communications Offences: A final report (Law Com No 399, 21 July 2021) https://assets.publishing.service.gov.uk/media/61ba022ad3bf7f05539de6f5/Modernising-Communications-Offences-2021-Law-Com-No-399.pdf.

Lovdata, Penal Code of Norway (Straffeloven), s 311 https://lovdata.no/dokument/NLE/lov/2005-05-20-28

Online Safety Act Explainer (Department for Digital, Culture, Media & Sport, 2024) https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

PROTECT Act of 2003, Pub L No 108–21, 117 Stat 650 (codified in part at 18 USC §§ 2251–2260A) https://www.congress.gov/bill/108th-congress/senate-bill/151.

Protection of Children Act 1978 (UK) https://www.legislation.gov.uk/ukpga/1978/37.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [General Data Protection Regulation] OJ L119/1 https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Strafgesetzbuch (German Criminal Code, StGB), § 184b https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1902

Swedish Penal Code, ch 16, s 10a https://www.government.se/4a7ad6/contentassets/c68c6dfce58b4045b6d825ba0a97db4e/the-swedish-penal-code

UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment (2 March 2021) UN Doc CRC/C/GC/25 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

United Nations, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, vols 2171–2171 (2000) https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/crc-sale.pdf.

Cases

Ashcroft v. Free Speech Coalition, 535 US 234 (2002) https://supreme.justia.com/cases/federal/us/535/234/.

New York v. Ferber, 458 US 747 (1982) https://supreme.justia.com/cases/federal/us/458/747/.