

SYNTHETIC CHILD SEXUAL ABUSE MATERIAL AND INDIAN CRIMINAL LAW REFORM: A COMPARATIVE STUDY OF UK AND US LEGISLATIVE RESPONSES

D. Sankar*, Safoora Ahad

Vellore Institute of Technology, Chennai, Tamil Nadu, India

*sankar.d@vit.ac.in

Abstract

The rapid development of artificial intelligence (AI) has transformed various sectors, but it has also created serious challenges for child protection, particularly in the digital environment. One of the most alarming developments is the emergence of AI-generated child sexual abuse material (CSAM), which enables the creation, possession, manipulation, and dissemination of abusive content without requiring direct physical contact with a child. This phenomenon forms part of a broader problem involving synthetic media, including non-consensual intimate deepfakes (NCID), which constitute a form of image-based sexual abuse and disproportionately affect women and girls. In India, the urgency of this issue is reflected in the rising number of cybercrimes against children. The National Crime Records Bureau (2022) reported a significant increase in such offences, while the National Cyber Crime Reporting Portal documented approximately 1.94 lakh CSAM-related cases by April 2024. India's legal response to online child sexual abuse is primarily governed by the Protection of Children from Sexual Offences (POCSO) Act, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023. However, these frameworks were not specifically designed to address the legal and evidentiary complexities posed by AI-generated, synthetic, morphed, and tool-assisted CSAM. The absence of explicit provisions on AI-generated CSAM creates gaps in enforcement, classification, liability, and regulatory oversight. This study adopts a qualitative doctrinal research methodology to examine the adequacy of India's existing legal framework in addressing AI-generated CSAM. It critically analyses relevant statutory provisions, legal principles, and policy gaps, while also conducting a comparative assessment of recent legislative developments, including the UK's Crime and Policing Act, 2026, and the U.S. Take It Down Act, 2025. Drawing on these comparative insights, the study argues that India must strengthen its legal, regulatory, and technological infrastructure to respond effectively to emerging AI-enabled cyber threats and to ensure robust protection of children in the digital age.

Keywords: Artificial Intelligence; Child Sexual Abuse Material; Child Protection; Synthetic Media; Indian Cyber Law.

A. Introduction

Child sexual abuse (CSA) is a globally serious public health issue, especially in this digital age. The World Health Organisation (WHO) defines CSA as "instances where children or adolescents are subjected to sexual contact that they cannot comprehend, agree to, or be prepared for developmentally, or when it violates legal laws or social norms" (WHO, 2017). Experiencing abuse during childhood can negatively affect children's physical and mental well-being (Hailes et al., 2019). It may lead to long-term consequences, including challenges with sexual functioning (Gewirtz-Meydan & Lahav, 2020) and compulsive sexual behaviours, such as problematic pornography use (Abajobir et al., 2017). These issues affect individuals, families, communities,

and all aspects of children's lives, including their physical, social, emotional, behavioural, and cognitive development. Even when children recognise that something is wrong, they are often unable to articulate or disclose their experiences to trusted individuals. Furthermore, when disclosures do occur, victims frequently encounter inadequate support systems, particularly when the perpetrator is a family member or close acquaintance, such as a sibling, cousin, stepfather, or teacher (Latiff et al., 2024; Nasution et al., 2025; Nugroho et al., 2026).

The proliferation of digital technologies has fundamentally altered the nature of child sexual abuse (CSA) and exploitation. Smartphones, with their readily accessible cameras and video capabilities, enable the instantaneous creation and dissemination of exploitative imagery. This shift has eliminated the need for third-party involvement in image development and distribution, significantly lowering the barriers to production and circulation (Ciardha et al., 2026).

As of January 2023, India had 692 million internet users, approximately 30.4% of whom were children (Kemp, 2023). With the migration of more activities online following COVID-19 lockdowns, children now face increased risks. As many students attend classes and socialise online, they become vulnerable to sexual exploitation and grooming, particularly as abusers target these situations. The lack of in-person interactions with peers, combined with extended and unsupervised online activity, heightens children's exposure to potential dangers (Harris et al., 2021). The ease of access to encrypted messaging apps, peer-to-peer networks, and the dark web enables perpetrators to evade detection and distribute child sexual abuse and exploitation material (CSAM/CSEM) (Katharina, 2020).

The production, possession, and distribution of child sexual abuse material (CSAM) is a significant component of online child exploitation that inflicts life-altering harm on child victims. Defined as any visual depiction of a child engaged in real or simulated sexual acts, CSAM is an escalating threat to children worldwide (UNIN, 2024).

AI-generated CSAM can be categorised into two main types: AI-altered CSAM that involves actual children, and computer-generated images of children participating in explicit sexual activities (Parti & Szabó, 2024). This category includes "deepfakes," which are manipulative creations made without the victim's consent, leading to psychological distress, social stigma, and significant privacy and security issues (Noviantama & Rahman, 2025). Although AI holds great promise for aiding law enforcement, it also poses numerous risks that could threaten basic freedoms and violate human rights, such as privacy, equality, and non-discrimination. The capability of generative AI to produce such material presents a major obstacle to law enforcement efforts;

A significant issue arises when AI-generated CSAM does not involve any identifiable real child, sparking debates about whether it is a "victimless offence" (Lazaridou, 2025). This situation calls for immediate academic investigation to address it properly (Lazaridou, 2025). Specialists are questioning whether existing laws, which criminalise CSAM involving actual children, can be effectively applied to AI-generated CSAM, especially when no real child can be identified (Kokolaki & Fragopoulou, 2025). As AI-driven content manipulation becomes more common, it will become increasingly challenging to differentiate AI-generated CSAM from material that depicts real children engaged in sexual activities.

The Protection of Children from Sexual Offences (POCSO) Act, 2012, aims to combat the sexual exploitation and abuse of minors by imposing strict penalties and ensuring a child-friendly judicial process. Nevertheless, similar to many conventional sexual offence statutes, the Act primarily concentrates on safeguarding actual children who have suffered abuse.

The issue with entirely AI-generated CSAM lies in its lack of connection to a real child victim. When no identifiable child is involved, applying the existing provisions of the POCSO Act becomes challenging. Laws that target offences against real children may struggle to address content in which the depicted child is not real (Parti & Szabó, 2024). The debate over AI-generated

CSAM being a “victimless offence” (Lazaridou, 2025) directly questions the fundamental basis of laws like POCSO, which are designed to protect actual victims from harm.

The Bharatiya Nyaya Sanhita 2023 (BNS) includes Section 294, which penalises the sale, distribution, or public display of obscene materials. Furthermore, Section 295 forbids the sale, distribution, or exhibition of obscene content to minors.

The Information Technology (IT) Act, 2000, particularly Section 67B, deals with child sexual abuse material (CSAM). Nonetheless, when it comes to artificial intelligence, there seems to be a notable “legal vacuum” in regulation, especially regarding deepfakes in India. This study suggests that the current AI regulations are inadequate for comprehensive governance, particularly in terms of technical details, implementation, and oversight of AI (Noviantama & Rahman, 2025). Likewise, the present legal framework and policies do not adequately cover the evolving nature of AI-driven technology, especially in the realm of AI-powered geo-spatial surveillance. India presently lacks the necessary resources and capacity to effectively tackle AI-generated CSAM.

The urgent need to revise the IT Act arises from the threat posed by deepfakes, which generate deceptive content without the consent of those affected, resulting in psychological distress, social stigma, and significant threats to personal privacy and security (Furizal et al., 2025). In the absence of specific regulations, there is a potential for technology to be misused and for legal clarity to be compromised (Talha et al., 2026).

The concept of “no identifiable real child” significantly transforms the way legal systems, which are traditionally designed to protect actual victims, need to adapt. Fully AI-generated CSAM is defined as computer-created images of children involved in sexual activities without the participation of any real child. This distinction calls for a reassessment of how criminalisation is applied, as the potential harm from not fully criminalising AI-generated CSAM demands immediate academic attention.

Additionally, the growing sophistication of AI technology makes it challenging to distinguish between authentic and artificially created content. This technical issue complicates the enforcement and prosecution under current laws, which may require evidence of a real victim or an actual act of abuse.

This article adds to the expanding discussion on technology-driven child sexual exploitation by critically analysing the new threat posed by AI-generated child sexual abuse material (CSAM) in the context of Indian law. The study underscores the shortcomings of current laws, such as the Protection of Children from Sexual Offences Act, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, in dealing with synthetic, altered, and AI-assisted child exploitation content. By integrating comparative insights from the Crime and Policing Act, 2026, and the TAKE IT DOWN Act, 2025, the article offers a modern legal examination of global reactions to AI-facilitated sexual abuse. The research further contributes by suggesting legal and technological reforms to enhance India's cyber governance and child protection systems against emerging digital threats.

B. Method

This study employs a qualitative doctrinal research design to examine the legal frameworks governing AI-generated child sexual abuse material (CSAM). The study relies on secondary sources, including statutes, judicial decisions, government reports, policy documents, journal articles, and international legal instruments. It critically analyses existing statutory provisions, legal principles, and policy gaps within the Indian legal system. The research also includes a comparative evaluation of legal frameworks in the United Kingdom and the United States. The USA and the UK have been selected for comparison because both jurisdictions have recently introduced progressive legal measures specifically targeting AI-generated sexual abuse content. The UK legislation is relevant for tool-based prevention, while the US legislation is relevant for victim-centred takedown obligations and platform accountability.

This study aims to assess the applicability of the Protection of Children from Sexual Offences Act and the Information Technology Act, 2000, in addressing AI-generated child sexual abuse and exploitation material (CSAM/CSEAM). It further seeks to identify and analyse the normative and legal gaps within the Indian legal framework concerning synthetic, morphed, and AI-generated CSAM/CSEAM, particularly in relation to enforcement, definitional clarity, and regulatory adequacy. In addition, this study evaluates comparative legal approaches reflected in the Crime and Policing Act, 2026, and the TAKE IT DOWN Act, 2025, to propose suitable legal reforms for India that remain consistent with the principles of legality, proportionality, due process, child protection, and platform accountability.

C. Results and Discussion

1. The Emergence of AI-Generated CSAM and Its Growing Threat to Child Protection

The emergence of AI-generated CSAM represents an evolving challenge in India within a broader context, with technological advancements and legal ambiguities (Garg & Shukla, 2025). Historically, researchers have focused on physical sexual abuse, while recent studies have highlighted the growing threat posed by digitally driven and online exploitation.

Puhan et al. (2025) emphasise the challenges of cross-border jurisdiction and implementation issues within the Indian digital environment related to the distribution of CSAM on the Dark Web. They have mentioned that the proliferation of digital technologies facilitates the spread of abusive content, complicating legal enforcement and victim protection efforts. They discuss the challenges faced by AI and cryptocurrencies while facilitating cyber child sexual abuse and describe an illegal ecosystem that leverages pseudo-pornography and other digital tools that exploit victims. This study highlights the increasing number of online abuse mechanisms and the importance of a sophisticated legal framework to cover these emerging threats (Jamaludin, 2026). This study reveals that AI-generated CSAM, often indistinguishable from genuine content, complicates detection and enforcement efforts and raises concerns about the effectiveness of current laws.

Historically, India has had a high prevalence of child sexual abuse. A study estimates that a child under 16 is raped every 155 minutes, and one in every ten children experiences sexual abuse at some point (Singh et al., 2014). Despite the rising number of cases, research on AI-generated abusive material remains limited, even though such content is used as a cybercrime commodity and is a growing concern. The legislation in India, as discussed by Belur et al. (2015), aims to safeguard children under 18 from sexual offences, but the rapid evolution of digital abuse methods challenges the effectiveness of existing laws and their implementation. Iravani (2011) notes that harassment and sexual abuse are only beginning to enter the national consciousness, and that the country lacks a sufficient body of research on the subject. India also reveals a significant gap in research and awareness. Yousafzai (2018) states the long-term psychological and social impacts of child sexual abuse, underscoring the need for robust prevention and intervention strategies, which are currently hampered by technological challenges.

Child Sexual Abuse Material (CSAM) refers to any digital or visual content—such as photos, videos, or other media—depicting the sexual abuse, exploitation, or coercion of children. This content, whether real or simulated, may include videos of sexual acts with children and is used by sexual predators to gratify their sexual desires or for economic sexual exploitation. CSAM, also known as child pornography, encompasses the production, sharing, or possession of any sexually explicit material involving minors, perpetuating a cycle of exploitation and harm. This illegal material spreads across digital platforms, including email, messaging apps, and online forums, making it challenging to protect children online. As minors increasingly use digital devices, they are at greater risk of exposure to CSAM, which can significantly harm their mental and sexual well-being. The creation of CSAM directly harms children by subjecting them to abuse and trauma. Furthermore, each instance of viewing or sharing this material further victimises the child,

compounding their suffering. The widespread availability of CSAM remains a critical concern due to its severe and enduring consequences for survivors.

The advent of AI has transformed the landscape of child sexual exploitation. Generative AI tools can produce realistic images and videos depicting child sexual abuse, complicating the identification and prosecution of offenders. Research indicates that the distribution of CSAM in Indian cyberspace has reached alarming levels, with millions of illegal files circulating online (Gautam et al., 2022). The anonymity provided by the internet, particularly on the dark web, further exacerbates the situation (Natalis & Djohan, 2025).

AI-based child sexual abuse material (CSAM), or 'deepfakes,' can generally be categorised into two types: (a) AI-created CSAM depicting fictional children in sexual situations and (b) AI-altered CSAM, which involves modifying images and videos of real children to create sexually explicit content (Krishna et al., 2024). Deepfakes represent a distinct category of synthetic media. The term, a portmanteau of 'deep learning' and 'fake,' describes media generated through deep learning algorithms to synthesise an individual's likeness in video, image, or audio formats (van der Sloot & Wagenveld, 2022). The Oxford English Dictionary defines a deepfake as "Any of various media, especially a video, that has been digitally manipulated to convincingly replace one person's likeness with that of another, often used maliciously to depict someone engaging in actions they did not perform" (Oxford English Dictionary, 2024). One of the initial legal definitions of deepfakes is offered by the recently enacted EU AI Act, which characterizes them as "AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person to be authentic or truthful." While various computational methodologies can be utilised to generate deepfakes, the fundamental principle involves employing artificial intelligence tools to create media that either depict or substitute the likeness of an actual individual (Krishna et al., 2024).

Non-consensual intimate deepfakes are referred to as "intimate deepfakes created and/or disseminated without the subject's consent" (Umbach et al., 2024). This terminology highlights the lack of consent, drawing a parallel with other sexual offences. Consent is considered absent either when the subject has not consented to the creation of the deepfake or when they have consented to its creation but not its dissemination. This term, NCIDs, refines earlier academic terms such as "fake involuntary pornographic deepfakes" and "non-consensual synthetic intimate imagery" (Graham, 2026). Furthermore, the term NCIDs is broad enough to include intimate content that is not explicitly sexual, such as partial or non-sexual nudity, which can still cause significant harm. This paper argues that the creation, distribution, and threatened distribution of non-consensual intimate deepfakes (NCIDs) should incur criminal liability.

Technological advancements have rendered many existing laws on non-consensual intimate material ineffective in addressing the novel issue of digital manipulation. For instance, if an image depicts a nude individual with the victim's actual face but digitally fabricated genitalia, current legal codes may not apply because the intimate body part isn't the victim's own. Therefore, it is crucial for states to provide victims with appropriate legal recourse against the creators and distributors of such intrusive content and to update legislation to keep pace with the rapidly evolving technological landscape.

As technology advances each year, the dangers associated with AI-Generated (GenAI) CSAM are escalating, as reflected in the global statistics. In 2024, the dark web saw the emergence of over 3,500 new AI-generated criminal child sexual abuse images, with a realism rate of 90%, making them indistinguishable from actual CSAM (IWF, 2025). The increasing seriousness of this AI dilemma was recently underscored by Operation Cumberland, one of Europol's initial large-scale investigations involving AI-generated CSAM, which extended across 19 countries and resulted in 25 arrests globally (Europol, 2025).

India is well aware of this looming crisis, as there has been a surge in generated CSAM cases, with the numbers escalating from 44 registered incidents in 2018 to 1,171 in 2022. Although these

figures only account for officially documented cases, the actual numbers continue to rise, particularly as free and enhanced open-source models emerge in the tech world with each passing day (NCRB, 2025).

A child protection charity reported that AI-generated child sexual abuse and exploitation images are on the rise, with 3,512 such images detected on a dark web platform in a single month. Of those, Category A images, which are the most serious, increased 10% compared to the same month the previous year. Researchers note that AI-generated child sexual abuse material often contains highly realistic visual features, making it difficult to distinguish from images depicting real victims.

In a one-month observational study of a dark web forum for child sexual abuse material (CSAM), the Internet Watch Foundation (IWF) identified 20,254 AI-generated images. After evaluating 11,108 of these images, the IWF determined that 27% directly violated United Kingdom laws against CSAM. Nine months later, a subsequent report indicated a substantial increase in images depicting penetrative sexual activity posted on the same forum, activity classified as the most egregious form of CSAM under UK law (IWF, 2023). In 2025 alone, 8,029 AI-generated images and videos were identified as depicting realistic child sexual abuse (IWF, 2024).

The National Centre for Missing & Exploited Children (NCMEC), a US-based non-profit organisation, initiated the Cyber Tipline to report CSAM on online platforms both in the USA and globally. In 2022, Cyber Tipline received over 32 million reports of suspected child sexual exploitation, with 99% of these reports originating from Electronic Service Providers (ESPs). Among the countries that submitted reports, five ESPs accounted for 90% of the submissions: Facebook, Instagram, Google, WhatsApp, and Omegle. Facebook reported the highest number of cases.

According to this report, India emerged as the largest contributor to CSAM found online, with the volume of CSAM uploaded from India increasing by 185.5% (from 1.98 million to 5.67 million CSAM) between 2019 and 2022 (Jivesh & Gupta, 2025). As per the National Crime Records Bureau (NCRB) report, there were 1823 cases in total of children's cybercrimes in 2022, accounting for a significant increase from the 1376 cases reported the last year. This highlights the shocking rise of such crimes in India. The recent surge in the prevalence and scale of AI-driven CSAM has garnered public attention, particularly following Europol's arrest of two dozen individuals involved in an international criminal network distributing AI-driven CSAM, marking a pioneering operation of its kind (Reuters, 2025).

Furthermore, certain websites on the dark web employ integrated models to facilitate the generation of CSAM, in addition to numerous platforms offering services to "nudify" images (Murphy, 2023). Additionally, AI models capable of operating "offline" are utilised to produce such images (Foundation, 2023). Images of well-known children and victims of CSA available on the internet are employed to train these AI models, given the substantial dataset involving these individuals (IWF, 2025). The endeavours of perpetrators are further bolstered by manuals available on dark web forums and guidance from fellow perpetrators on refining the generation of CSAM. Consequently, the current dark web-facilitated AI CSAM environment has allowed offenders to form collectives, enhance their resilience, and reinforce each other's criminal activities.

Additionally, many AI-generated child sexual abuse materials (CSAM) reuse images of known victims, further traumatising them, while others exploit images of well-known minors, effectively creating new victims (Belanger, 2023). However, AI-driven CSAM poses an even greater danger because it doesn't always depend on pre-existing abusive content—it can be generated without any prior photos. There have been reports of minors producing deepfake nude images of their peers.

2. From Synthetic Images to Real Harm: The Impact of AI-Generated CSAM on Children

A pressing issue is the application of AI-generated CSAM to portray actual children—whether they are children who have previously suffered abuse for the creation of CSAM or those who have not been victimised before. It has been reported that AI technology is being utilised to produce images that resemble past victims of sexual abuse. As a result, even children who have been taken out of harmful situations or have their identifiable CSAM images hashed for detection continue to suffer from new types of synthetic exploitation (IWF, 2024). AI technology facilitates the production of explicit content from non-explicit images, including those of celebrity children or minors whose pictures are innocently posted on social media (IWF 2023, 2024), as well as children whose images are captured in public settings. This content might be entirely new, such as images generated using diffusion models specifically adjusted to portray a particular child, or it might involve the application of “nudification” software (Gibson et al., 2025), deepfake technology, or other AI-driven methods to alter photographs taken with a camera, resulting in explicit images of specific children.

AI CSAM is increasingly used not just as a passive tool but also as a means to enable new forms of coercion and exploitation. Recent reports indicate that manipulated or entirely synthetic images are employed alongside other AI technologies in grooming practices. Offenders use fabricated explicit content to desensitize children, threaten them with exposure, or further exploit them (Quayle, 2016). A rising issue is the increase in sexual extortion cases involving AI-generated images (Milmo & editor, 2025), where synthetic sexual content is utilized to manipulate or coerce minors into creating real sexually explicit material, paying money, or granting access to sensitive information as a form of payment (Thiel et al., 2023).

These attacks might consist of entirely synthetic content, material captured by cameras, or a mix of both—for example, when AI-generated or altered content is used to pressure victims into producing new, authentic images that are later misused. They could also involve mere threats to fabricate AI-altered content (Patchin & Hinduja, 2020). Perpetrators of online sexual extortion exhibit a range of motivations, including those with a sexual interest in minors and those driven by financial gain, who may target young individuals as part of broader cybercrime and scam activities (O'Malley & Holt, 2022).

The merging of different cybercrime categories poses a risk of introducing a broader array of AI-driven methods—such as voice cloning to boost credibility—for executing large-scale sexual exploitation. Although the involvement of AI in sexual extortion schemes is still developing, the psychological effects on minors are already well-established. Victims frequently suffer from trauma-related symptoms like shame, helplessness, anxiety, suicidal thoughts, and trust issues (Ray & Henry, 2025). There have been several instances where sexual extortion has been associated with self-harm and suicide (Ray & Henry, 2025).

The proliferation of Child Sexual Abuse Material poses many serious psychological challenges, not only for the victims but also for the perpetrators and those involved in its detection and moderation. For victims, the psychological impact is deep and lasting. According to the literature, child sexual abuse survivors commonly report anxiety disorders, depression, and posttraumatic stress disorder (Pulverman et al., 2018). The trauma can make it challenging to develop healthy relationships or else accelerate cycles of intergenerational abuse (Widom et al., 2014). CSAM perpetrators also face major psychological dangers. Research has shown that offenders who have viewed CSAM are at an increased risk of suicidal ideation compared with the general population and other violent offenders (Kothari et al., 2021). The psychological impact of engaging in such material would render feelings of shame, guilt, and isolation, which in turn keep them from looking for help (Insoll et al., 2024).

Further, numerous risk factors lead to online child sexual abuse and exploitation. More generally, they are: (a) demographic variables of age, gender, disability, socio-economic status, and sexual orientation; (b) the type of online social interaction and activity, including use of chat

rooms and decisions or actions in relation to online chat, “sex talk,” or transmission of personal data; and (c) emotional vulnerability due to psychiatric morbidity and/or past abuse experiences (Quayle, 2016). Other risk factors include normative adolescent developmental patterns (Pharo et al., 2011), i.e., impulsive and risk-taking behaviour in general, increased awareness of sexuality, feeling sexual arousal, and, for some individuals, participation in sexual activity.

3. Existing Legal Framework in India

India’s legal framework for tackling online Child Sexual Abuse (OCSA) and Child Sexual Abuse/Exploitation Material (CSAM/CSEAM) is distributed across several laws, such as the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and rules concerning intermediary liability for online platforms. Although these laws offer crucial safeguards against online sexual exploitation, there are still notable doctrinal and technological shortcomings, especially in relation to AI-generated CSEAM, deepfake child abuse images, synthetic portrayals, virtual children, generative AI systems, automated distribution networks, and tools for prompt-based image creation. The table below provides a critical assessment of the scope, applicability, and limitations of India’s legal framework in the face of new digital and AI-driven forms of child sexual exploitation.

Table 1.
Scope and Limitations of India’s Legal Framework on Online Child Sexual Abuse and AI-Generated CSAM/CSEAM

Statute	Relevant Provisions	Scope	Gaps and Limitations
Protection of Children from Sexual Offences Act, 2012 (POCSO)	Sections 13–15	Sections 13–15 criminalise the use of children for pornographic purposes, possession, storage, transmission, and commercial use of child sexual abuse material. The Act also establishes special courts, child-friendly procedures, mandatory reporting obligations, rehabilitation measures, and enhanced procedural safeguards for child victims.	The Protection of Children from Sexual Offences (POCSO) Act, 2012, makes it a crime to use children to produce pornographic material and distribute, possess, or even create such material. The Act, however, is phrased in such a way that it assumes the presence of a real child, and it is unclear whether the synthetic or AI-generated content would be subject to the Act.
Information Technology Act, 2000 (as amended in 2008)	Sections 67A–67C, 67B	Sections 67A–67C criminalise publication, transmission, browsing, downloading, and circulation of sexually explicit electronic content. Section 67B specifically addresses child pornography by penalising electronic publication, distribution, advertisement, promotion, or browsing of sexually explicit material involving children. Section 67C imposes data retention obligations on intermediaries.	Section 67B lacks a clear definition of CSAM and does not account for synthetic or AI-generated material; largely reactive enforcement model.

Statute	Relevant Provisions	Scope	Gaps and Limitations
IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021	Rule 3(1)(b), Rule 4	Imposes due diligence obligations on intermediaries and social media platforms to remove unlawful content, retain user data, and cooperate with law enforcement agencies in relation to illegal online material, including CSAM.	No mandatory proactive detection of AI-generated CSAM; the notice-and-takedown approach is insufficient for rapidly proliferating synthetic material
Bharatiya Nyaya Sanhita, 2023 (formerly IPC, 1860)	Sections 294, 295, 77, 78, 79, 351	Sections 294–295 criminalise obscenity, sale, circulation, and exhibition of obscene materials. Sections 77–79 address voyeurism, stalking, harassment, and insulting modesty. These provisions may indirectly apply to the circulation of sexually explicit content online, including voyeuristic or exploitative digital material.	Obscenity-based framework inadequately captures sexual exploitation of children online; provisions are not child-specific
Judicial Interpretation	<i>Just Rights for Children Alliance v. S. Harish</i> (2024)	Clarified that possession and storage of CSAM constitute offences	Judicial guidance cannot substitute for explicit statutory reform; AI-generated material remains unaddressed

Source: Author's analysis based on the Protection of Children from Sexual Offences Act, 2012; Information Technology Act, 2000; IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Bharatiya Nyaya Sanhita, 2023; and *Just Rights for Children Alliance v. S. Harish* (2024)

The statutory framework outlined above illustrates that India has several legal tools to tackle various aspects of online child sexual exploitation and abuse. Judicial interpretation, notably in the case of *Just Rights for Children Alliance v. S. Harish* (2024) has broadened the scope of liability by identifying the viewing, possession, and constructive possession of CSAM/CSEAM as offences subject to punishment. Additionally, the Protection of Children from Sexual Offences Act 2012 includes provisions that criminalise the use of child sexual abuse material for pornographic purposes, as well as its possession, storage, transmission, and commercial exploitation. The Information Technology Act 2000 also imposes penalties for the publication or transmission of sexually explicit material involving a child in electronic form. However, there is ambiguity regarding whether AI-generated content is covered by this definition. This gap in definition poses challenges for prosecution and emboldens offenders who may exploit such technological loopholes with near impunity (Manoj et al., 2025).

Despite this, the framework remains mostly reactive and technologically outdated as AI systems rapidly advance. Current laws were mainly crafted to govern traditional electronic publication and the transmission of abusive content, rather than the synthetic media ecosystems driven by generative AI. As a result, there is considerable uncertainty surrounding fictional AI-generated children, stylised or animated portrayals, AI-generated avatars, synthetic abuse imagery not associated with identifiable minors, AI training datasets, prompt-based generation systems, and automated redistribution networks.

Additionally, the provisions under the Bharatiya Nyaya Sanhita 2023 still heavily depend on obscenity doctrines based on morality-driven regulation. Modern international approaches increasingly view CSAM/CSEAM not just as “obscene content,” but as evidence of child

exploitation, abuse, coercion, and systemic harm. Therefore, India needs a specific legislative framework to address AI-generated CSEAM, deepfake child abuse material, virtual child depictions, generative AI systems, and intermediary accountability in the age of artificial intelligence.

S. Harish vs. Inspector of Police

In recent judicial proceedings (S. Harish vs The Inspector of Police on 11 January, 2024), the Madras High Court, in the case of quashed charges, determined that downloading child pornography did not constitute an offence under Section 67B of the Information Technology (IT) Act, 2000. The court explicitly stated that the mere act of viewing child pornography was not an offence, as the accused had only downloaded and viewed it privately on his electronic device. The Madras High Court also referenced a judgment by the Kerala High Court, which held that viewing pornography in a private setting does not violate section 292 of the Indian Penal Code (IPC). This case involved the dismissal of a criminal case filed by the Aluva police in 2016 against a youth found watching pornographic material on his mobile phone at night on the roadside. The Madras High Court concluded that children watching pornographic material in private does not constitute an offence under the Information Technology Act, 2000, or the Protection of Children from Sexual Offences Act, 2012.

However, on 23 September 2024, a Division Bench comprising Chief Justice D.Y. Chandrachud and Justice J.B. Pardiwala in Just Rights for Children Alliance v. S. Harish (Just Rights For Children Alliance vs S. Harish on 23 September, 2024) held that the mere viewing, possession, and storage of material depicting minors engaged in sexual activity is an offense under the Protection of Children from Sexual Offences Act, 2012. This decision resolves a longstanding division among High Courts regarding whether “mere storage” of ‘child pornography’ constitutes an offence under Section 15 of the POCSO Act and Section 67B of the Information Technology Act, 2000 (‘IT Act’). Specifically, it overturned the Madras High Court’s decision in S. Harish v. Inspector of Police and Another (2024), which had quashed criminal proceedings against a POCSO accused, finding that downloading or watching ‘child pornography’ was not, per se, penalised under either the POCSO or the IT Act.

Justice Pardiwala emphasised the need to replace the term ‘child pornography’ with ‘child sexual exploitation and abuse material,’ which he argued more accurately reflects the nature of such crimes. He recommended that Parliament amend the POCSO Act to incorporate this terminology (Just Rights For Children Alliance vs S. Harish on 23 September, 2024).

Justice Pardiwala clarified the scope of Section 15 of the POCSO Act 2012, highlighting three distinct offences related to child pornography: Section 15(1) “failure to delete, destroy or report” that is in the possession of the accused. Section 15(2) penalises the actual transmission, propagation, or display of child pornography. Section 15(3) penalises the actual storage or possession of child pornography for commercial purposes. The intent behind the act is crucial for determining guilt under Section 15 of the POCSO ACT, 2012 (Patnaik , 2024).

Justice Pardiwala explained that under Section 15(1), the mens rea, or intent, must be inferred from the actus reus, specifically the act of possessing the material without reporting it. In each case, the facts and circumstances surrounding the acquisition of possession and the reasons for nondisclosure must be examined. According to this interpretation, mere possession of the material constitutes an offence under Section 15 unless it is deleted, destroyed, or reported by the accused.

Justice Pardiwala clarified that each provision within Section 15 operates independently. This interpretation rejects the alternative approach previously adopted by certain High Courts, which had construed the offences of possession and distribution as constituting a single offence. The Court noted that in cases of ‘child pornography,’ the victimisation of the minor commences with the sexual act and is further exacerbated by the recording of the act, the dissemination of photographs and videos, thereby creating a “ripple of trauma” for the child.

Justice Pardiwala proposed that the term "child sexual exploitative and abuse material" (abbreviated as 'CSEAM') is a more suitable designation for this egregious act, as opposed to "child pornography." He argued that the latter term diminishes the severity of victimisation by implying an association with pornography, which is a legal activity involving subjects who voluntarily participate and are capable of consenting to the conduct" (Patnaik, 2024).

The judgment strongly recommends that Parliament "seriously consider" amending the Protection of Children from Sexual Offences (POCSO) Act to replace the term 'child pornography' with 'Child Sexual Exploitation and Abuse Material' (CSEAM). It further urges the Union to contemplate enacting the proposed amendment through an ordinance to facilitate prompt action. Additionally, it has issued a directive to all courts to refrain from using the term 'child pornography' in judicial orders and judgments (Patnaik, 2024).

4. Addressing AI-Driven Child Sexual Exploitation Material (CSEAM) under Indian Law and the Gaps

The creation of AI-generated Child Sexual Exploitation and Abuse Material (CSEAM) based on a real child renders the creator legally liable under Section 14 for employing a child for pornographic purposes (Punishment for using a child for pornographic purposes (Section 14, POCSO 2012 Act). This is due to the adaptable and modifiable nature of CSEAM, which is considered illegal if it appears to depict a child. The generation of deepfakes or the application of online "nudifying" tools on images of real children constitutes an act of modifying or adapting images, thus qualifying as CSEAM involving that child. Even animated or seemingly fictional depictions can fall within this scope if they are based on real minors, as their appearance still suggests a depiction of a child.

The law also holds individuals accountable under Section 15 POCSO Act 2012 for storing pornographic material involving children if they access CSEAM via the internet, regardless of whether it is entirely AI-generated. If the AI-created images are indistinguishable from those of real children or appear to portray a minor, they are treated as CSEAM. This interpretation is supported by the apex court's decision, which expanded the definition of "possession" to include "constructive possession," thus encompassing digital access and storage.

Despite these possible meanings, there remains great uncertainty about how the current Indian laws apply to AI-created CSEAM. To begin with, although AI content that is created and does not exist in a real child may be considered to fall within the ambit of material that "appears to depict a child," the Protection of Children from Sexual Offences (POCSO) Act describes a "child" as a "person" below the age of eighteen years. This brings about doubts on whether CSEAM with non-existent children or virtual children can legally constitute child pornography under the Act. However, such material can potentially cause harm to society through the desensitization of audiences to the abuse of children (Seigfried-Spellar & Rogers, 2013), decreased psychological barriers to acting upon abusive tendencies (Russell & Purcell, 2006), the sexualisation of children, and eventual contributions to the growth of the child exploitation industry (National Association of Attorneys General, 2023)

The challenge of addressing AI-generated child sexual abuse material exists in a legal grey area where technology has outpaced legislation. While the unethical nature of such content may appear obvious, criminalising it is not straightforward. Current child pornography laws are based on the premise of identifiable child victims, creating a doctrinal gap when no real children are exploited in creating synthetic images. This ambiguity provides opportunities for offenders to exploit legal loopholes, while prosecutors grapple with inconsistent laws, evidentiary challenges, and constitutional constraints. The issue extends beyond merely updating legal definitions; it involves finding a balance between safeguarding free expression and technological progress and the imperative of protecting children.

Second, the label “computer-driven image” has limitations. The computer generation process is usually characterised by intentional human input, management, and imagination, while AI technologies can automatically create content without explicit human control. This difference makes legal classification more difficult.

The primary issue arises from the absence of a real victim in AI-generated CSAM. Traditional criminal law largely hinges on the notion of harm, asserting that a crime necessitates a victim who has suffered injury or exploitation. This fundamental aspect of harm is often cited by offenders and civil liberties advocates, who argue that synthetic material is merely fictional. Although subsequent legislation has sought to address this gap, the situation highlights an ongoing conflict: criminalising imaginary scenarios risks overgeneralization and censorship, yet failing to do so may promote their creation and societal harm. Jurisdictions adhering to a harm-based definition of CSAM risk exclude synthetic material from prosecution.

The challenges of prosecution are further complicated by issues related to detection and evidence. The increasing use of AI to generate CSAM makes it increasingly challenging to differentiate between artificial and real images, creating a significant hurdle for law enforcement. When forensic experts examine the offenders' materials, they face substantial difficulties in proving whether the images depict real children or are entirely artificial. This ambiguity in evidence can undermine prosecution efforts, as defence attorneys exploit these doubts to argue that no crime occurred. Additionally, there is a risk of false accusations, as legitimate yet stylised digital art might be misidentified as CSAM. Courts are often ill-equipped to address such technical questions, particularly in the absence of expert testimony or standardised forensic tools to analyse synthetic media (Sanchez et al., 2019).

The situation is further complicated by the cross-border nature of online distribution. AI-generated CSAM is often created in one jurisdiction and hosted on servers in different parts of the world. Different jurisdictions have varying legal standards, enabling criminals to operate without fear of consequences. For instance, someone in a country where synthetic CSAM is legal can distribute it to countries where it is prohibited, and law enforcement is powerless due to the principle of double criminality in extradition law. The lack of unified global standards thus creates jurisdictional loopholes that can be exploited.

The challenges of legal interpretation are compounded by the practical difficulties encountered in prosecuting and investigating CSEAM cases. These cases demand significant resources, including specially trained police officers, advanced digital tools, and dedicated cybercrime units — areas where India currently faces shortages. Additionally, the international nature of CSEAM, similar to other cybercrimes, creates jurisdictional challenges (Steel, 2026).

Online grooming, defined as the procedure through which online predators cultivate a deceptive sense of emotional closeness with minors, thereby facilitating the establishment of trust for subsequent exploitation (Odudu, 2024), remains an area inadequately addressed by Indian legislation. The data from the National Crime Records Bureau (NCRB) reveals a staggering 400% increase in incidents related to cyber pornography, cyberbullying, and cyberstalking involving children in connection with the Information Technology Act about online offences against minors during the period from 2019 to 2020. Within the aggregate of 842 recorded cases in 2020, a significant 738 cases pertained to the dissemination or transmission of sexually explicit materials involving minors.

Section 11(iv) of the POCSO Act addresses the utilisation of minors for pornographic endeavours; however, it does not explicitly criminalise the act of grooming itself, which entails a systematic psychological manipulation preceding the physical exploitation of a victim. The phenomenon referred to as the “invisible threat” by experts is characterised by predators establishing relationships with minors, predominantly via online gaming platforms, social media networks, and messaging applications, until a foundation of trust is cultivated, after which sexual content is introduced, explicit images are solicited, or the relationship is transitioned offline.

Various nations maintain that exploitation initiates well in advance of the perpetrator establishing physical contact with the minor. India's inability to acknowledge grooming as an independent criminal offence leaves children vulnerable at a juncture where intervention is of paramount importance.

5. International Perspective: Comparative Analysis of the UK and the USA Legislation

The comparative study of the United Kingdom and the United States does not simply aim to chronicle international statutory developments but focuses on identifying specific legislative mechanisms that can help bridge gaps in India's response to AI-generated CSAM. Both countries have moved beyond traditional, image-based conceptions of child sexual exploitation and have begun to legislatively anticipate harms arising from synthetic, deepfake, and AI-assisted abuse—a trajectory that remains absent in Indian law.

a. United Kingdom- Crime and Policing Act, 2026

The advent of AI has brought with it immense growth and harm. The ability to create explicit and abusive images of children through AI has become a pressing and deeply unsettling issue. Offenders are using these technologies to edit real images, produce new abusive material, and even blackmail victims into further exploitation. The Home Office introduced its Crime and Policing Bill, aimed at criminalising the possession and dissemination of information on using artificial intelligence (AI) for creating child sexual abuse material (CSAM). This bill was presented to Parliament on February 25, 2025, and received Royal Assent on 29 April 2026, and is now the Crime and Policing Act 2026. The Act makes the United Kingdom the world's first country to introduce new sexual abuse offences to safeguard children from AI image producers who use them for predatory purposes.

The Act makes criminal the following acts: possessing, creating, or distributing child sexual abuse material, and having AI manuals that guide people on how to use AI to abuse children. Imposing new obligations on online platforms to ensure that their systems and processes remove non-consensual intimate images as soon as reasonably practicable, and no later than 48 hours after receiving a report. The Crime and Policing Act seeks to make policing more efficient, more transparent, and stronger in public confidence. This wide-ranging Act covers several unrelated crimes, such as encouraging another to cause themselves serious harm and possession and distribution of a SIM card.

A report released in October 2023 by the Internet Watch Foundation has found the use of artificial intelligence in the creation of child sexual abuse material. This study examined more than 20,000 AI-created images that were shared on a dark web forum in one month. 3,000 images out of these showed criminal offences involving child sexual abuse (Mildred, 2025).

While existing statutes criminalise child sexual abuse material, the government acknowledges a legislative gap, as current laws do not address the “production, possession, distribution, or advertisement of digital models or files intended for the creation of CSAM.” The Act seeks to address this gap by establishing a new offence related to the creation, adaptation, possession, supply, or offer to supply a child sexual abuse image-generator. The Act defines a child “sexual abuse image-generator” as “any entity (including any service, program, or information in electronic form) designed or adapted for the creation or facilitation of CSA images.” Upon conviction on indictment, this offence would be subject to a penalty of up to five years' imprisonment, a fine, or both.

The Act aims to fill a gap in the current legal framework regarding the possession and sharing of information on how to make AI-generated child sexual abuse images. Precisely, the Act aims to modify Section 69 of the Serious Crime Act by “creating a new crime for the possession of guidance or instruction on how to make child sexual abuse images. On

conviction on indictment, this offence would carry a maximum penalty of three years' imprisonment, a fine, or both".

Furthermore, the proposed legislation seeks to criminalise engaging in specific internet activities with the intent to facilitate child sexual exploitation and abuse. The Act delineates "relevant internet activity" as including the provision of an internet service; the maintenance or assistance in maintaining an internet service provided by another entity; the administration, moderation, or control of access to content on an internet service; or the facilitation of content sharing on an internet service. "This provision is intended to encompass individuals commonly referred to as 'moderators' or 'administrators' of websites containing child sexual abuse material (CSAM). Upon conviction on indictment, this offence is subject to a penalty of up to ten years' imprisonment and/or a fine".

The proposed legislation would empower the Border Force to conduct scans of electronic devices for images related to child sexual abuse (CSA), contingent upon the presence of reasonable grounds for suspicion that an individual is carrying such material. According to the accompanying Explanatory Notes, reasonable suspicion may be established under several conditions, including the individual being listed on an Interpol notice related to potential CSA offenders that has been uploaded to the UK Border Watch List, being a registered sex offender in the UK, or when intelligence is received from the National Crime Agency (NCA), domestic police forces, or international counterparts. Additional indicators may include the possession of CSA-related paraphernalia in one's luggage or a travel history that aligns with repeated visits to regions designated by the Secretary of State as high-risk areas for child sexual exploitation involving UK nationals or residents. The legislation would also obligate individuals to comply with device scans and to facilitate access—such as by unlocking their devices—while requiring that such scans be conducted using technology approved by the Secretary of State.

The introduction of a new statutory aggravating factor addressing grooming behavior in the sentencing of specified sexual offenses committed against individuals under the age of 18. The criminalization of the creation, modification, distribution, or provision of tools and services designed to generate or facilitate the generation of purported intimate images of individuals, commonly known as "nudification tools." The imposition of new obligations on online platforms to ensure that non-consensual intimate images are removed from their systems as expeditiously as possible and, in any event, no later than 48 hours after a report is received.

The legislation mandates that ministers assign a registry, such as the Revenge Porn Helpline, for the purpose of disseminating information regarding non-consensual intimate images to internet service providers. Subsequent to an evaluation, ministers will possess the authority, through secondary legislation, to enact additional provisions concerning the registry's operation. This includes the imposition of obligations on internet service providers to share intimate image hashes with the registry.

b. Reforms from the UK Crime and Policing Act, 2026

India may draw several important lessons from the proposed provisions of the United Kingdom's Crime and Policing Act 2026. In particular, India should consider expressly criminalising artificial intelligence tools, software, and digital models that are specifically designed, developed, or modified to create child sexual abuse material (CSAM), including child sexual exploitation and abuse material (CSEAM).

Although the existing legal frameworks under the Protection of Children from Sexual Offences Act 2012 and the Information Technology Act 2000 criminalise the creation, possession, and dissemination of CSAM, they do not adequately address AI-generated or

synthetic child sexual abuse material. Nor do they clearly prohibit the development and circulation of technologies specifically intended to facilitate its production.

The introduction of a distinct criminal offence covering the creation, possession, distribution, provision, or promotion of AI-enabled tools designed to generate such material would strengthen India's capacity to respond to emerging technological threats. Such an offence would also enable preventive intervention before abusive material is actually produced, thereby addressing not only the resulting content but also the technological infrastructure that facilitates its creation and dissemination.

Secondly, India could implement legislative measures that criminalise the possession or distribution of manuals, instructions, or technical guidance designed to aid in the generation of AI-produced Child Sexual Abuse Material (CSAM). Such legislative measures would acknowledge that not only the resultant material but also the dissemination of technical knowledge that facilitates its creation plays a significant role in the broader framework of online child exploitation.

Thirdly, the model established in the United Kingdom underscores the imperative to impose liability on individuals who wilfully enable online child sexual exploitation via internet platforms, websites, encrypted groups, or digital services. Indian legislation could likewise contemplate the introduction of explicit liability for administrators, moderators, or operators of online platforms who deliberately facilitate the distribution of Child Sexual Abuse Material (CSAM) or Child Sexual Exploitation Material (CSEAM) or provide the necessary infrastructure for such illicit activities. This measure would enhance accountability within digital environments where child sexual abuse material is increasingly proliferated through organised online networks.

India may consider granting law enforcement agencies limited, judicially supervised digital investigation powers, specifically for cases involving transnational child sexual exploitation. Given the increasing use of encrypted devices and cloud-based storage, narrowly tailored powers to examine digital devices in high-risk situations could significantly assist investigations. However, unlike broad enforcement powers, any such mechanism in India must strictly adhere to the constitutional right to privacy, as recognised in *Justice K. S. Puttaswamy v. Union of India*. It should also incorporate robust safeguards, including judicial oversight, necessity, proportionality, adherence to data protection standards, and effective remedies against misuse (Dey & Dey, 2025)

India must, however, exercise caution against over-criminalisation. Criminal liability should specifically target intentional conduct involving exploitation, facilitation, or the deliberate creation of abusive synthetic content, thus avoiding the inadvertent penalisation of legitimate technological research, cybersecurity, or lawful AI development. While the UK approach demonstrates the importance of addressing emerging harms, India must balance child protection objectives with constitutional safeguards for free expression, privacy, due process, and proportionality. Consequently, instead of just broadening the definition of CSAM/CSEAM, India could gain from implementing an inclusive legal structure that explicitly covers AI-generated abusive content, criminal facilitation via digital platforms, and the improper use of generative technologies, all while ensuring strong procedural safeguards and protection against capricious enforcement.

c. USA- The Enactment of the TAKE IT DOWN Act, 2025

The Tools to Address Known Exploitation by Immobilising Technological Deepfakes on Websites and Networks Act, or TAKE IT DOWN Act, 2025, is a US Federal Statute aimed at preventing the distribution of non-consensual intimate images or "revenge porn," as well as deepfake content that is shared through websites and social media (Ayerza et al., 2026; Nwuda, 2026; Sundberg, 2025). These technological forgeries are often made with artificial

intelligence tools. The law was presented by Senator Ted Cruz in June 2024, passed overwhelmingly with bipartisan support in both houses of Congress, and was enacted into legislation when President Donald Trump signed it on May 19, 2025 (Greeno, 2025).

The TAKE IT DOWN Act, 2025, criminalises the online dissemination of both real and synthetic sexually explicit content without consent, marking the first federal statute to explicitly address this issue (U.S. Congress, 2025). Under the law, social media platforms and other websites are mandated to remove such material—including AI-generated deepfakes—within 48 hours of a victim’s request. Violators face substantial penalties, including imprisonment.

Critically, the Act contains a good faith protection for covered platforms, protecting them from liability if they take down or disable reported non-consensual deepfake content even if later review finds the content did not technically infringe the law. This provision protects platforms in good faith carrying out takedown notices from legal action by content providers, thus promoting proactive moderation while addressing free expression concerns.

Section 3 of the Take It Down Act, 2025 requires covered online services to adopt certain content takedown procedures. The law requires all applicable services to develop procedures - within one year after enactment - allowing for individuals (or their representatives) to request takedown of non-consensual private visual depictions. With the signing date of the Act as May 19, 2025, this notice-and-takedown regime is to become lawfully enforceable as of May 19, 2026, providing a twelve-month grace period for platforms to design compliant infrastructures.

The Act defines a “covered platform” in broad terms to include any website, online service, online application, or mobile application that is accessible to and serves the public. This definition is not limited to traditional social media platforms, but also extends to other digital spaces where users are able to create, upload, exchange, or distribute content. A platform may fall within this category if it primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files. The scope of the definition is therefore designed to capture various forms of online interaction where harmful intimate visual depictions may be shared. In addition, the Act also covers platforms whose ordinary course of trade or business involves publishing, curating, hosting, or making available non-consensual intimate visual depictions. This means that liability is not confined to platforms that merely host user content, but may also apply to services that actively manage or distribute such material as part of their regular operations (Sen. Cruz, 2025)

The Act establishes a procedural framework that requires covered platforms to respond to removal requests only when such requests are considered “valid” under the law. This requirement is important because it creates a formal standard that individuals must satisfy before a platform is legally obligated to act. A removal request is regarded as valid when it is made in writing and contains specific information that allows the platform to verify the request and identify the relevant content. First, the request must include the physical or electronic signature of the individual submitting it, or the signature of an authorised representative acting on that individual’s behalf. This requirement helps confirm that the request is genuinely made by the affected person or by someone legally permitted to represent them. Second, the request must provide sufficient identification of the intimate visual depiction that is being challenged. This means that the individual must give enough information to enable the covered platform to locate the material, such as a URL, account name, post details, image description, or any other relevant identifying information. Without this information, platforms may struggle to determine which content must be reviewed or removed, particularly when similar or duplicate materials are widely circulated.

In addition, the individual making the request must include a brief statement explaining their good-faith belief that the intimate visual depiction was created, shared, or distributed

without consent. This element does not require the individual to prove the lack of consent at the initial stage, but it does require them to make a clear assertion that the material is non-consensual. The good-faith standard is designed to prevent abusive or false takedown requests while still ensuring that victims are not placed under an excessive evidentiary burden. The request must also include the individual's contact information, allowing the platform to communicate with the requester if clarification is needed or if the platform must confirm the status of the removal process. Once a covered platform receives a valid removal request, the Act imposes a strict obligation to remove the identified content within 48 hours. This short timeframe reflects the urgent nature of intimate image-based abuse, where delay can significantly increase the harm suffered by the victim. The rapid spread of digital content means that even a brief period of inaction can result in repeated viewing, downloading, reposting, and further dissemination across multiple platforms.

The Act also requires covered platforms to make reasonable efforts to identify and remove any known identical copies of the same material. This obligation extends the platform's responsibility beyond the specific link or post identified in the original request. It recognises that non-consensual intimate images are often reposted, mirrored, or redistributed after the original content has been removed. By requiring platforms to address identical copies, the Act seeks to reduce the repeated victimisation that occurs when harmful material continues to circulate online despite an initial takedown. However, the phrase "reasonable efforts" leaves some room for interpretation, as platforms may differ in their technological capacity, resources, and moderation systems (Sen. Cruz, 2025).

The Act mandates that covered platforms display clear and conspicuous notice (e.g., via a dedicated webpage) explaining their notice-and-takedown procedures in plain language, including instructions for submitting removal requests. Non-compliance constitutes an unfair or deceptive practice under Section 18(a)(1)(B) of the Federal Trade Commission Act (FTCA), enforceable by the FTC through civil penalties, injunctions, or consumer redress (Federal Trade Commission, 2025).

Critically, liability applies only to platforms that fail to remove unlawful content—not those that erroneously remove lawful material in good faith. Section 3(a)(4) of the Act "expressly shields platforms from legal claims arising from such good-faith removals, even if the content is later deemed permissible. This balance incentivises proactive moderation while mitigating over-enforcement risks" (Sen. Cruz, 2024).

Section 2 "establishes felony penalties for knowingly disseminating non-consensual intimate imagery or AI-generated forgeries ("digital forgeries") of minors or adults through digital platforms, with limited exceptions. The provision targets content creators rather than platforms, imposing fines and potential 3-year imprisonment for violations. "Digital forgery" is broadly defined to include hyper-realistic AI-generated content indistinguishable from authentic material (Sen. Cruz, 2024).

The legislation responds to the escalating risks posed by deepfake technology, a tool increasingly exploited to generate non-consensual, hyper-realistic explicit imagery—disproportionately targeting women and minors. In many cases, victims remain unaware of such fabricated content until irreversible reputational, emotional, or psychological damage has occurred. By instituting uniform federal regulations and mandating prompt removal of illicit material, the law remedies a critical legal void that previously denied victims effective avenues for redress.

d. Reforms from the US TAKE IT DOWN ACT, 2025

India could adopt several significant reforms inspired by the US TAKE IT DOWN Act, 2025, particularly in establishing a victim-centred legal framework to address AI-generated sexual abuse material and non-consensual intimate imagery. In contrast to traditional criminal

laws that primarily emphasise punitive measures after an offence, the US model integrates criminalisation with rapid content-removal obligations, platform accountability, and mechanisms for victim redress. Incorporating these elements could substantially enhance India's current legal framework under the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, and the Information Technology.

First, India may consider introducing a statutory notice-and-takedown mechanism specifically for AI-generated CSAM/CSEAM and non-consensual intimate imagery. At present, Indian law imposes due diligence obligations on intermediaries under the IT Rules. Still, there is no dedicated statutory mechanism requiring rapid removal of synthetic sexual abuse material upon a victim's request. Adopting a time-bound takedown framework, similar to the 48-hour requirement under the TAKE IT DOWN Act, 2025, could help minimise ongoing harm caused by the viral dissemination of deepfake sexual content. Such a mechanism could be integrated with India's cybercrime reporting portal and coordinated through specialised cybercrime units and child protection authorities.

Secondly, India might consider implementing more explicit obligations concerning platform accountability. The model adopted by the United States imposes direct responsibilities on "covered platforms" to create accessible procedures for lodging complaints, articulate transparent policies for content removal, and expeditiously eliminate unlawful content. Indian legislation could similarly mandate that intermediaries and social media platforms establish dedicated reporting mechanisms for AI-generated sexual abuse material, including deepfakes depicting child sexual abuse. Such measures would enhance accessibility for victims, particularly minors, who frequently encounter procedural obstacles when attempting to report online abuse.

Thirdly, the good-faith immunity granted to platforms by the TAKE IT DOWN Act, 2025, offers a crucial insight for India. This Act shields platforms from legal liability when they act in good faith to remove reported exploitative material, even if the content is subsequently found to be lawful. Adopting similar protective measures in India could foster proactive content moderation, expedite removal processes, and alleviate intermediaries' concerns about potential litigation. However, these measures must be meticulously defined to prevent arbitrary censorship or the excessive removal of legally permissible content.

Furthermore, the Indian legal framework would benefit from explicitly criminalising the distribution of AI-generated sexually explicit deepfakes involving both minors and adults. While current Indian legislation penalises obscene and sexually explicit materials, ambiguity exists regarding AI-generated content, particularly when no real child is involved in its creation. A distinct statutory provision that explicitly recognises AI-generated representations of sexual abuse as illegal would effectively mitigate this legal ambiguity and align Indian law with evolving technology.

The TAKE IT DOWN Act, 2025 emphasises victim-centred remedies. To this end, Indian reforms should prioritise measures such as simplified complaint procedures, robust confidentiality protections, and comprehensive psychological support for victims. Additionally, there is a need for expedited coordination among law enforcement agencies, online intermediaries, and child welfare authorities. Victims of deepfake abuse often endure significant reputational and emotional harm, which can persist long before criminal proceedings are finalised. Therefore, rapid content removal and immediate support mechanisms are crucial, complementing criminal prosecution rather than waiting for its conclusion.

However, India must carefully integrate these reforms into its constitutional framework. Any mandatory takedown regime, for instance, must incorporate robust procedural safeguards to prevent misuse, false complaints, and excessive censorship. Crucially, legislative consideration will be needed to determine the appropriate enforcement authority, whether it

be the Ministry of Electronics and Information Technology, CERT-In, cybercrime units, or an independent digital safety body. Furthermore, takedown obligations must always remain proportionate and consistent with constitutional protections for freedom of speech and privacy, as guaranteed by Articles 19 and 21 of the Indian Constitution (Mandloi, 2025).

The crucial lesson India can draw from the TAKE IT DOWN Act 2025 is that effectively combating AI-generated sexual exploitation demands more than just criminalisation. It also requires an integrated framework encompassing rapid victim redress, platform accountability, clear procedures, intermediary cooperation, and balanced safeguards against the abuse of enforcement powers.

6. Legal and Institutional Reforms for Addressing AI-Generated Child Sexual Abuse Material in India

The most urgent requirement is to modernise legal definitions. Current laws, such as India's POCSO Act, 2012, and Section 67B of the Information Technology Act, 2000, assume that actual victims, photographs, or videos exist. This creates ambiguity regarding AI-generated content. To clarify, legislatures must extend the definition of child sexual abuse material. It should include morphed, animated, and artificial images of underage children in sexual situations, regardless of whether an actual child exists. The justification for this expansion goes beyond preventing direct harm. It also seeks to prevent the normalisation of child exploitation in society. Countries like the USA and the United Kingdom already criminalise the possession and distribution of virtual child pornography. Similar laws could be adapted into Indian law.

The definition of criminal responsibility requires reform concerning AI-generated child sexual abuse material (CSAM). Currently, the absence of a "genuine child" in such content allows offenders to rationalise their acts as victimless. However, this approach overlooks a significant societal harm: it risks normalising these materials, blurring the distinction between real abuse and simulated content, and thereby validating deviant sexual inclinations. Therefore, the statute must be amended to explicitly declare the creation, sale, and possession of AI-generated CSAM illegal *per se*. This would allow the act itself to infer criminal intent, shifting the burden of proof to the defendant. Such an approach aligns with existing anti-terrorism and drug laws, which acknowledge that severe societal harms can justify legal action without requiring direct, identifiable victimisation. Introducing a separate statute that defines and criminalises cyber grooming—communicating electronically with a child for sexual grooming purposes—will ensure early intervention, preventing abuse from escalating to physical contact or the production of imagery.

All social media companies and digital platforms operating in India must be subject to mandatory laws on powerful content moderation, CSAM proactive detection using hash-matching technologies like PhotoDNA, age-verification mechanisms, and full-time reporting to law enforcement agencies within a set timeframe of all detected abuses (Das & Choudhury, 2022). Dedicated child cybercrime investigation teams must have forensic training in every district. These teams need access to advanced technology tools for evidence gathering. Robust procedures for cross-border collaboration with international enforcement agencies, such as INTERPOL and the National Centre for Missing & Exploited Children, are also essential (V V et al., 2025).

The government will integrate age-appropriate digital safety education into school curricula nationwide, focusing particularly on rural and marginalised communities, where children are most vulnerable. This initiative will also include training for teachers, parents, and community leaders to recognise indicators of potential online exploitation (Abed et al, 2025).

CWC and JJB should establish specific protocols for supporting survivors of digital exploitation. These protocols should include mental health professionals trained in technology-facilitated abuse and offer long-term aftercare that addresses the profound psychological impacts of knowing that abusive material can be virtually permanent.

The manuscript outlines several proposed legal and institutional reforms, including amendments to the POCSO Act, the establishment of specialized cybercrime units, enhanced AI detection systems, and rapid takedown mechanisms. However, implementing these recommendations poses significant practical challenges. The success of such reforms relies on financial resources, technological infrastructure, trained personnel, and effective inter-agency coordination.

For example, creating specialized cybercrime units and AI-assisted monitoring systems would necessitate considerable government investment in digital infrastructure, forensic laboratories, and ongoing training for law enforcement officers. Additionally, developing effective AI detection tools for synthetic CSAM introduces technical challenges related to algorithmic accuracy, encrypted platforms, cross-border jurisdictional issues, and the risk of false positives that could mistakenly classify lawful content as illicit.

Implementing rapid takedown mechanisms can face procedural and jurisdictional challenges, especially when online platforms or servers are based outside of India. Additionally, smaller states and rural areas may struggle with limited resources for maintaining dedicated cyber forensic capabilities. While these recommendations are legally desirable and essential for enhancing child protection frameworks, their effective implementation must be phased and supported by sufficient funding, international cooperation, public-private partnerships, and capacity-building initiatives (Sayyed, 2024, 2024). Future policy development should also incorporate cost-benefit assessments, pilot implementation models, and periodic evaluations to ensure the operational sustainability of these reforms.

D. Conclusion

Child sexual abuse (CSA) constitutes a pervasive and grievous offence, exacerbated by advancements in generative artificial intelligence (AI). These technological developments facilitate the creation, dissemination, and misuse of synthetic child sexual abuse material (CSAM). The profound and enduring consequences of CSA necessitate both legislative and societal intervention, particularly as AI technology diminishes the barriers for malicious actors to produce harmful content, such as non-consensual intimate deepfakes (NCID) and algorithmically altered images.

Indian legislation currently provides limited protection against online child sexual exploitation through the Protection of Children from Sexual Offences Act, 2012, and the Information Technology Act, 2000. These statutes primarily address the creation, possession, and distribution of child sexual abuse material. However, they were enacted before the emergence of generative artificial intelligence and are inadequate for comprehensively addressing AI-generated Child Sexual Exploitative and Abuse Material (CSEAM), synthetic abuse imagery, and technology-driven exploitation. The ruling in *Just Rights for Children Alliance v. S. Harish* has significantly strengthened the legal framework by recognising the criminal nature of possessing and viewing CSEAM and by advocating for a shift from the term “child pornography” to “CSEAM.” Nonetheless, judicial interpretation alone cannot substitute for the necessity of comprehensive legislative reform.

The comparative study elucidates two distinct yet complementary reform strategies. The United Kingdom’s approach emphasises preventive criminalisation through regulation of artificial intelligence tools, image generators, facilitation networks, and online exploitation infrastructure. Conversely, the United States’ TAKE IT DOWN Act, 2025 adopts a victim-centred strategy that prioritises rapid takedown requirements, platform accountability, and protections against non-consensual synthetic imagery. Both approaches illustrate that contemporary regulation of AI-driven child sexual exploitation transcends traditional obscenity laws.

The analysis further indicates that deficiencies in enforcement and procedural mechanisms substantially undermine current legal responses. Issues such as jurisdictional fragmentation,

evidentiary challenges, a lack of technological expertise, and constraints in cross-border cooperation persistently hinder effective investigation and prosecution. Digital forensic evidence often presents authentication difficulties; judicial authorities may lack the technical capacity to evaluate AI-generated material, and prosecutions frequently falter due to challenges related to admissibility or the inability to establish exploitative intent. The anonymity afforded by the dark web and encrypted communication technologies further emboldens offenders and complicates enforcement efforts.

India necessitates an integrated legal framework that explicitly criminalises AI-generated child sexual exploitation and abuse material (CSEAM) and exploitative synthetic content. This framework should also reinforce the obligations of intermediaries and platforms, modernise evidentiary and procedural mechanisms, and enhance cyber forensic and judicial capacities. Furthermore, these reforms must incorporate constitutional safeguards concerning privacy, freedom of expression, proportionality, and due process to prevent the misuse of enforcement powers.

REFERENCES

- Abajobir, A. A., Kisely, S., Maravilla, J. C., Williams, G., & Najman, J. M. (2017). Gender Differences in the Association Between Childhood Sexual Abuse and Risky Sexual Behaviours: A Systematic Review and Meta-Analysis. *Child Abuse & Neglect*, 63, 249–260. <https://doi.org/10.1016/j.chiabu.2016.11.023>
- Ayerza, J. M., Lee, J. R., & Darcy, K. M. (2026). An Examination of U.S. Image-Based Sexual Abuse Legislation: An Assessment of Federal and State Responses to Nonconsensual Dissemination of Intimate Images. *International Journal of Police Science & Management*, 28(2), 126–148. <https://doi.org/10.1177/14613557261447761>
- Belanger, A. (2023, November 2). *Teen Boys Use AI to Make Fake Nudes of Classmates, Sparking Police Probe*. Ars Technica. <https://arstechnica.com/tech-policy/2023/11/deepfake-nudes-of-high-schoolers-spark-police-probe-in-nj/>
- Belur, J., & Singh, B. B. (2015). Child Sexual Abuse and The Law in India: A Commentary. *Crime Science*, 4(1), 26. <https://doi.org/10.1186/s40163-015-0037-2>
- Ciardha, C. Ó., Buckley, J., & Portnoff, R. (2026). AI-Generated Child Sexual Abuse Material: What's the Harm? *AI & SOCIETY*. <https://doi.org/10.1007/s00146-026-02932-y>
- Das, S., & Choudhury, P. (2022). International Child Sexual Exploitation Database to Fight Child Sexual Abuse and Artificial Intelligence. In N. Singh Malik, E. A. Gromova, S. Gupta, & B. Balusamy (Eds), *Legal Analytics: The Future of Analytics in Law* (1st edn, pp. 235–244). Chapman & Hall/CRC. <https://doi.org/10.1201/9781003215998-18>
- Dey, A., & Dey, S. K. (2025). Leveraging AI in Prevention and Protection of Women Against Cybercrime in India: A Paradigm Shift of Criminal Law in the Making. In M. Chakraborty, S. P. Chakraborty, A. Penteado, & V. E. Balas (Eds.), *Proceedings of 5th International Ethical Hacking Conference* (Vol. 1148, pp. 307–330). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-8457-8_20
- Europol. (2025, February 28). *25 Arrested in Global Hit Against AI-Generated Child Sexual Abuse Material*. <https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material>

- Federal Trade Commission. (2025, July). *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*. Federal Trade Commission. <https://www.ftc.gov/about-ftc/mission/enforcement-authority>
- Foundation, I. W. (2023). *How AI is Being Abused to Create Child Sexual Abuse Imagery*. Internet Watch Foundation London.
- Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., & Sharkawy, A.-N. (2025). Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review. *Social Sciences & Humanities Open*, 12, 101882. <https://doi.org/10.1016/j.ssaho.2025.101882>
- Garg, D., & Shukla, D. (2025). Combatting AI-Generated Child Sexual Exploitation and Abuse Material: An Analysis of India's Techno-Legal Response. *Indian Journal of Law and Technology*, 21(1), 1-27. <https://doi.org/10.55496/SZWH4909>
- Gautam, S. K., Khajuria, H., Gupta, R. R., & Nayak, B. P. (2022). Recent Trends in Child Sexual Abuse Material (CSAM) Distribution in Indian Cyberspace: *International Journal of Cyber Warfare and Terrorism*, 12(1), 1–15. <https://doi.org/10.4018/IJCWT.297857>
- Gewirtz-Meydan, A., & Lahav, Y. (2020). Sexual Functioning Among Childhood Sexual Abuse Survivors From an Attachment Perspective. *The Journal of Sexual Medicine*, 17(7), 1370–1382. <https://doi.org/10.1016/j.jsxm.2020.03.014>
- Gibson, C., Olszewski, D., Brigham, N. G., Crowder, A., Butler, K. R. B., Traynor, P., Redmiles, E. M., & Kohno, T. (2025). Analyzing the AI Nudification Application Ecosystem. *34th USENIX Security Symposium (USENIX Security 25)*, 1–20. <https://www.usenix.org/conference/usenixsecurity25/presentation/gibson>
- Graham, C. (2026). Fake Images, Real Harm: A Case for Criminalising Non-consensual Intimate Deepfakes. *Victoria University of Wellington Law Review*, 56(2), 159–192. <https://doi.org/10.26686/vuwlr.v56i2.10758>
- Greeno, T. (2025). Take It Down or Take It Too Far? The Legal Fallout of New Online Takedown Powers. *North Carolina Journal of Law & Technology*, 27(2), 201–236. <https://scholarship.law.unc.edu/ncjolt/vol27/iss2/2/>
- Hailes, H. P., Yu, R., Danese, A., & Fazel, S. (2019). Long-Term Outcomes of Childhood Sexual Abuse: An Umbrella Review. *The Lancet Psychiatry*, 6(10), 830–839. [https://doi.org/10.1016/S2215-0366\(19\)30286-X](https://doi.org/10.1016/S2215-0366(19)30286-X)
- Harris, M., Allardyce, S., & Findlater, D. (2021). Child Sexual Abuse and Covid-19: Side Effects of Changed Societies and Positive Lessons for Prevention. *Criminal Behaviour and Mental Health*, 31(5), 289–292. <https://doi.org/10.1002/cbm.2214>
- Insoll, T., Soloveva, V., Bethencourt, E. D., Ovaska, A. K., Nurmi, J., Paju, A., Aaltonen, M., & Vaaranen-Valkonen, N. (2024). Factors Associated with Help-Seeking Among Online Child Sexual Abuse Material Offenders: Results of an Anonymous Survey on the Dark Web. *Journal of Online Trust and Safety*, 2(4), 1-43. <https://www.tsjournal.org/index.php/jots/article/view/205>
- Iravani, M. R. (2011). Child Abuse in India. *Asian Social Science*, 7(3), 150–153. <https://doi.org/10.5539/ass.v7n3p150>

- IWF. (2024). *How AI Is Being Abused to Create Child Sexual Abuse Imagery*. Internet Watch Foundation. <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/>
- IWF. (2025). *IWF Annual Report 2024*. Internet Watch Foundation (IWF). <https://www.iwf.org.uk/annual-data-insights-report-2024/>
- Jamaludin, A., Anggraeni, H. Y., Noval, S. M. R., Sari, R. A. W., Sonjaya, S., & Fikri, A. M. (2026). Propagation of AI-Generated Child Sexual Abuse Material as a Cybercrime Commodity in Indonesia. *Oñati Socio-Legal Series*, 16(3), 1189–1206. <https://doi.org/10.35295/osls.iisl.2579>
- Jivesh, S., & Gupta, P. (2025). Legal Implications of Child Sexual Abuse Materials: Combating Online Exploitation. *International Journal of Law Management & Humanities*, 8(2), 3048–3070. <https://doi.org/10.10000/IJLMH.119409>
- Kokolaki, E., & Fragopoulou, P. (2025). *Unveiling AI's Threats to Child Protection: Regulatory efforts to Criminalize AI-Generated CSAM and Emerging Children's Rights Violations* (Version 1). arXiv. <https://doi.org/10.48550/ARXIV.2503.00433>
- Kothari, R., Key, R., Lawrenson, J., Squire, T., Farnham, F., & Underwood, A. (2021). Understanding Risk of Suicide among Perpetrators Who View Child Sexual Abuse Material (CSAM). *Journal of Forensic and Legal Medicine*, 81, 102188. <https://doi.org/10.1016/j.jflm.2021.102188>
- Krishna, S., Dubrosa, F., & Milanaik, R. (2024). Rising Threats of AI-Driven Child Sexual Abuse Material. *Pediatrics*, 153(2), e2023063954. <https://doi.org/10.1542/peds.2023-063954>
- Latiff, M. A., Fang, L., Goh, D. A., & Tan, L. J. (2024). A systematic Review of Factors Associated with Disclosure of Child Sexual Abuse. *Child Abuse & Neglect*, 147, 106564. <https://doi.org/10.1016/j.chiabu.2023.106564>
- Lazaridou, M. (2025). *Schrödinger's Crime: AI-Generated Child Sexual Abuse Material as a Victimless Offense* [Master's thesis, Utrecht University]. <https://studenttheses.uu.nl/handle/20.500.12932/48359>
- Mandloi, P. (2025). AI and Machine Learning: Revolutionizing the Fight Against Online Child Sexual Abuse Material (CSAM). In V. B. Gupta, S. K. Shandilya, F. Ortiz-Rodríguez, & J. L. Martinez-Rodríguez (Eds.), *Business Intelligence, Computational Mathematics, and Data Analytics* (pp. 30–48). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-87511-3_3
- Manoj, D., James, R. I., Kumaran, S., Devnath, G. P., Varughese, B. T., Arakkal, A. L., & Johnson, L. R. (2025). Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation. *Child Protection and Practice*, 4, 100088. <https://doi.org/10.1016/j.chipro.2024.100088>
- Mildred, B. (2025). Non-Consensual Intimate Deepfakes as a Form of Digitally Altered Online Child Sexual Exploitation and Abuse Material: A Review of the South African Legislative Position. *Child Abuse Research in South Africa*, 26(1), 22–40. https://doi.org/10.10520/ejc-carsa_v26_n1_a2
- Milmo, D., & editor, D. M. G. technology. (2025, March 20). More Than 110 Child Sextortion Attempts Reported Each Month to UK Police Forces. *The Guardian*.

<https://www.theguardian.com/uk-news/2025/mar/20/children-teenagers-sex-tortion-uk-national-crime-agency-campaign>

- Murphy, M. (2023, December 8). Apps That Use AI to Undress Women in Photos Soaring in Use. *Bloomberg.Com*. <https://www.bloomberg.com/news/articles/2023-12-08/ai-nudify-apps-that-undress-women-in-photos-soaring-in-use>
- Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2025). Addressing Deepfake Pornography and the Right to be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, 38(7), 2489–2517. <https://doi.org/10.1007/s11196-025-10265-0>
- Natalis, A., & Djohan, N. H. (2025). Cybersex Trafficking: Legal Challenges and Protection for Women and Children in Indonesia. *International Cybersecurity Law Review*, 6(3), 421–456. <https://doi.org/10.1365/s43439-025-00149-1>
- National Association of Attorneys General. (2023, September 5). *54 Attorneys General Call on Congress to Study AI and Its Harmful Effects on Children*. National Association of Attorneys General. <https://www.naag.org/policy-letter/52-attorneys-general-call-on-congress-to-study-ai-and-its-harmful-effects-on-children/>
- Noviantama, D., & Rahman, A. A. (2025). Deepfake: A Review from The Victimology Perspective. *Contemporary Issues in Criminal Law*, 1(2), 107–128. <https://doi.org/10.20885/CICL.vol1.iss2.art1>
- Nugroho, M. S., Hardiyanti, M., & Mahoro, J. C. G. (2026). When Men Are Victims: Power, Hegemonic Masculinity, and the Epistemic Limits of Justice in Indonesian Sexual Violence Law. *Jurnal Hukum Progresif*, 14(1), 201–240. <https://doi.org/10.14710/jhp.14.1.201-240>
- Nwuda, C. (2026). Systemic Failure and Synthetic Abuse: Regulating Nonconsensual Deepfakes Under the Take It Down Act. *DePaul Journal of Art, Technology & Intellectual Property Law*, 36(1), 103–167. <https://via.library.depaul.edu/jatip/vol36/iss1/5/>
- Odudu, Q. (2024). *Child Abuse: The Emerging Role of The Internet And Technology* (SSRN Scholarly Paper No. 4996057). Social Science Research Network. <https://doi.org/10.2139/ssrn.4996057>
- O'Malley, R. L., & Holt, K. M. (2022). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. *Journal of Interpersonal Violence*, 37(1–2), 258–283. <https://doi.org/10.1177/0886260520909186>
- Oxford English Dictionary. (2024). *Deepfake*, *n*. Oxford University Press. Oxford English Dictionary. <https://doi.org/10.1093/OED/7847968874>
- Parti, K., & Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws*, 13(6), 67. <https://doi.org/10.3390/laws13060067>
- Patchin, J. W., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse*, 32(1), 30–54. <https://doi.org/10.1177/1079063218800469>
- Pharo, H., Sim, C., Graham, M., Gross, J., & Hayne, H. (2011). Risky Business: Executive Function, Personality, and Reckless Behavior During Adolescence and Emerging Adulthood. *Behavioral Neuroscience*, 125(6), 970–978. <https://doi.org/10.1037/a0025768>

- Puhan, S., Kumar, A., Mishra, Y. R., R, C. C., Das, A., & Gupta, Y. C. (2025). Cross-Border Jurisdiction and IP Enforcement Challenges in Dark Web Distribution of Child Sexual Abuse Material. *Journal of International Commercial Law and Technology*, 6(1), 507–513. <https://doi.org/10.61336/Jiclt/25-01-46>
- Pulverman, C. S., Kilimnik, C. D., & Meston, C. M. (2018). The Impact of Childhood Sexual Abuse on Women's Sexual Health: A Comprehensive Review. *Sexual Medicine Reviews*, 6(2), 188–200. <https://doi.org/10.1016/j.sxmr.2017.12.002>
- Quayle, E. (2016). *Researching Online Child Sexual Exploitation and Abuse: Are There Links Between Online and Offline Vulnerabilities?* (Method Guide 7). Global Kids Online. <https://researchonline.lse.ac.uk/id/eprint/71260/>
- Ray, A., & Henry, N. (2025). Sextortion: A scoping review. *Trauma, Violence, & Abuse*, 26(1), 138–155. <https://journals.sagepub.com/doi/abs/10.1177/15248380241277271>
- Russell, D. E. H., & Purcell, N. J. (2006). Exposure to Pornography as a Cause of Child Sexual Victimization. In N. E. Dowd, D. G. Singer, & R. F. Wilson (Eds), *Handbook of Children, Culture, and Violence* (pp. 59–84). SAGE Publications, Inc. <https://doi.org/10.4135/9781412976060.n4>
- Sanchez, L., Grajeda, C., Baggili, I., & Hall, C. (2019). A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM). *Digital Investigation*, 29, S124–S142. <https://doi.org/10.1016/j.diin.2019.04.005>
- Sayyed, H. (2024). Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges. *Cogent Social Sciences*, 10(1), 2343195. <https://doi.org/10.1080/23311886.2024.2343195>
- Seigfried-Spellar, K. C., & Rogers, M. K. (2013). Does Deviant Pornography Use Follow a Guttman-Like Progression? *Computers in Human Behavior*, 29(5), 1997–2003. <https://doi.org/10.1016/j.chb.2013.04.018>
- Sen. Cruz, T. [R-T. (2024, December 4). *Text - S.4569 - 118th Congress (2023-2024): TAKE IT DOWN Act* [Legislation]. (2024-06-18). <https://www.congress.gov/bill/118th-congress/senate-bill/4569/text/is>
- Sen. Cruz, T. [R-T. (2025, May 19). *S.146 - 119th Congress (2025-2026): TAKE IT DOWN Act* [Legislation]. (2025-01-16). <https://www.congress.gov/bill/119th-congress/senate-bill/146>
- Singh, M. M., Parsekar, S. S., & Nair, S. N. (2014). An Epidemiological Overview of Child Sexual Abuse. *Journal of Family Medicine and Primary Care*, 3(4), 430–435. <https://doi.org/10.4103/2249-4863.148139>
- Steel, C. M. S. (2026). Child Sexual Exploitation Material: Investigative and Legal Challenges with Generative Artificial Intelligence. *Victims & Offenders*, 21(3), 555–573. <https://doi.org/10.1080/15564886.2025.2532541>
- Sundberg, T. K. (2025). Federalizing NCII Regulation: The Take It Down Act's Approach to Criminalization, Platform Liability, and Threats to Disseminate. *Georgia Law Review*, 59(3), 1207–1232. <https://digitalcommons.law.uga.edu/glr/vol59/iss3/9/>
- Talha, M., Irshad, N. U. N., Rehman, U. U., Gill, O. A., & Imtiaz, A. (2026). AI-Generated Child Sexual Abuse Material: A Threat to Pediatric Psychiatry Datasets and Diagnostic Accuracy.

- Clinical Child Psychology and Psychiatry*, 31(2), 844–846.
<https://doi.org/10.1177/13591045251399699>
- Thiel, D., Stroebel, M., & Portnoff, R. (2023). *Generative ML and CSAM: Implications and Mitigations*. Stanford Internet Observatory and Thorn. <https://doi.org/10.25740/jv206yg3793>
- Two dozen arrested in international swoop for links to AI-made child sex abuse images. (2025, February 28). *Reuters*. <https://www.reuters.com/world/europe/two-dozen-arrested-distributing-ai-generated-child-abuse-images-2025-02-28/>
- Umbach, R., Henry, N., Beard, G. F., & Berryessa, C. M. (2024). Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries. *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, CHI '24*, 1–20. <https://doi.org/10.1145/3613904.3642382>
- V V, V., Venugopal, B., & N, R. S. (2025). A Socio-Technological Approach to Addressing Child Sexual Abuse: Prevalence Trends, Forensic AI Tools, and Policy Implications in India and USA. *2025 First International Conference of Advances in Engineering and Computing Technologies for Sustainable Development (AECTSD)*, 1–5. <https://doi.org/10.1109/AECTSD65988.2025.11411090>
- van der Sloot, B., & Wagenveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. *Computer Law & Security Review*, 46, 105716. <https://doi.org/10.1016/j.clsr.2022.105716>
- Widom, C. S., Czaja, S., & Dutton, M. A. (2014). Child Abuse and Neglect and Intimate Partner Violence Victimization and Perpetration: A Prospective Investigation. *Child Abuse & Neglect*, 38(4), 650–663. <https://www.sciencedirect.com/science/article/pii/S0145213413003438>
- Yousafzai, A. W. (2018). Child Abuse: Are We Doing Enough to Prevent It? *Khyber Medical University Journal*, 10(1), 1–2. <https://doi.org/10.35845/kmu.j.2018.18148>