Page 2086 - 2100

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

AI-Generated Child Sexual Abuse and Exploitation Material (CSAEM): Evaluating the Adequacy of India's Child Protection Framework in the Generative AI Era

NINGAWAA SHAMRAO SHINDE[*] AND SHARDUL HEMANT MAKHARE[**]

ABSTRACT

The rapid advancement of generative artificial intelligence has created new challenges for child protection by enabling the production of realistic Child Sexual Abuse and Exploitation Material (CSAEM) without necessarily involving the direct abuse of an identifiable child. Deepfake technology, AI-generated imagery, and image-manipulation tools have challenged traditional legal understandings of victimhood and criminal liability. These create new risks for children through image-based sexual abuse, grooming, and the normalisation of child sexual exploitation. Against this backdrop, this paper examines whether India's existing child-protection framework is capable of responding to the challenges posed by AI-generated CSAEM. It analyses the constitutional framework, the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, recent judicial developments, and relevant international child-rights standards. The paper argues that although India's existing legal framework is sufficiently broad to address several forms of AI-generated CSAEM, it remains inadequate to respond to the distinctive harms associated with generative AI. Uncertainty surrounding fully synthetic child depictions, limited obligations for AI developers and digital platforms, and the absence of a preventive, child-centred regulatory approach continue to create significant legal gaps. The paper also lays down reforms that move beyond traditional victim-based regulation towards a child-centred governance framework that places greater emphasis on prevention, and the protection of children's rights in digital environments.

Keywords: *AI-generated CSAEM, Child Rights, Generative AI, Deepfakes, POCSO, Child Protection, Synthetic Victimisation*

[*] Author is a PhD Scholar at Sant Gadge Baba Amravati University, Amravati, Maharashtra, India.
[**] Author is a Student at National Law University, Nagpur, Maharashtra, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The rapid expansion of generative artificial intelligence (AI) has transformed the creation, distribution, and consumption of digital content. Publicly accessible AI systems can now generate highly realistic images, videos, and audio from simple text prompts, placing sophisticated content creation within reach of ordinary users.[1] While these developments have created opportunities in education, research, and the creative industries, they have also enabled new forms of online abuse. Among the most concerning is the emergence of AI-generated Child Sexual Abuse and Exploitation Material (CSAEM).[2]

Traditionally, the production of CSAEM required the direct involvement of a child, and legal frameworks developed on the assumption that an identifiable child had been photographed or recorded in sexually exploitative circumstances.[3] Generative AI challenges this premise. Image-generation models, deepfake technologies, and AI-assisted editing tools can now produce sexualised depictions of children without a camera and, in some instances, without involving an identifiable child.[4] Existing photographs of children can also be manipulated into sexually explicit images through widely available nudification and deepfake applications without the child's knowledge or consent.[5,6]

The rapid growth of such technologies has become a significant concern for child-protection agencies and law-enforcement authorities worldwide. AI-generated CSAEM is increasingly circulating through online platforms and dark-web networks, while open-source models and commercially available tools have substantially lowered the barriers to creating and distributing exploitative material.[7] What was once a technologically demanding process has become accessible to ordinary users through open-source tools and commercial applications.[8] These developments raise concerns not only about the normalisation of child sexual exploitation but

[1] INTERNET WATCH FOUNDATION, *Harm Without Limits: AI Child Sexual Abuse Material Through the Eyes of Our Analysts* (AI CSAM Report, March 2026).
[2] UNICEF, *Artificial Intelligence and Child Sexual Abuse and Exploitation* (Issue Brief, February 2026).
[3] Dhruv Garg and Dedipyaman Shukla, *Combatting AI-Generated Child Sexual Exploitation and Abuse Material: An Analysis of India's Techno-Legal Response*, 21(1) INDIAN JOURNAL OF LAW AND TECHNOLOGY (2025), doi: 10.55496/szwh4909.
[4] Emmanouela Kokolaki and Paraskevi Fragopoulou, *Unveiling AI's Threats to Child Protection: Regulatory Efforts to Criminalize AI-Generated CSAM and Emerging Children's Rights Violations*, arXiv:2503.00433 [cs.CY] (March 1, 2025).
[5] UNICEF, *supra* note 2.
[6] Caoilte Ó Ciardha, John Buckley and Rebecca S. Portnoff, *AI-Generated Child Sexual Abuse Material: What's the Harm?*, AI & SOCIETY (2026), doi: 10.1007/s00146-026-02932-y.
[7] INTERNET WATCH FOUNDATION, *supra* note 1.
[8] Kokolaki and Fragopoulou, *supra* note 4.

 [ISSN 2581-5369]

also about the re-victimisation of survivors, the misuse of children's images, and the growing difficulty of identifying and investigating AI-generated abuse.[9]

The harms associated with AI-generated CSAEM extend beyond the creation of illegal content. Synthetic material can facilitate grooming, sextortion, coercion, and image-based sexual abuse, while children whose images are manipulated into explicit content may suffer serious psychological, social, and reputational harm.[10] These consequences demonstrate that the issue cannot be viewed solely through the lens of criminal law. It is equally a child-rights issue that implicates children's dignity, privacy, safety, and overall development.[11]

India's response to child sexual exploitation is anchored principally in the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023.[12] In addition, the Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish*[13] recognised that such material should be understood as evidence of abuse and exploitation rather than as a form of pornography.[14] Together, these measures provide a foundation for addressing online child sexual exploitation.

These instruments were, however, largely developed before the emergence of generative AI, and the primary statutes do not expressly address fully synthetic child depictions, AI-enabled image manipulation, developer responsibility, or platform accountability.[15]

Against this backdrop, this paper examines whether India's existing child-protection framework is adequate to address AI-generated CSAEM. Through a doctrinal analysis it argues that although the existing framework is sufficiently broad to apply to many forms of AI-generated CSAEM, it remains inadequate to address the distinctive harms posed by generative AI. The paper therefore advocates a shift from a predominantly victim-based approach towards a child-centred governance framework.

II. Conceptualising AI-Generated CSAEM

Child Sexual Abuse and Exploitation Material (CSAEM) has traditionally referred to visual content depicting the sexual abuse or exploitation of children. For many years, laws were built

[9] Internet Watch Foundation, *supra* note 1.
[10] UNICEF, *supra* note 2.
[11] UNICEF, *supra* note 2.
[12] The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012); The Information Technology Act, 2000 (Act 21 of 2000), s. 67B; The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 95, 96 and 295.
[13] *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716 (Sup. Ct. India, Sept. 23, 2024).
[14] *Just Rights for Children Alliance*, *supra* note 13.
[15] Ankit Yadav, *Protecting Dignity in Cyberspace: A Critical Analysis of Judicial Responses to Digital Sexual Exploitation in India*, 3(4) LawFoyer International Journal of Doctrinal Legal Research 2116 (2026), doi: 10.70183/lijdlr.2025.v03.215.

 [ISSN 2581-5369]

on the assumption that such material originated from the direct abuse of an identifiable child who was photographed, recorded, or otherwise depicted in sexually exploitative circumstances.[16] The development of generative AI has complicated this understanding by enabling the creation of sexualised depictions of children without conventional image-production processes and, in some cases, without the involvement of a real child at all.[17]

The terminology used to describe such material has also evolved. International organisations, child-rights advocates, and courts have increasingly rejected the expression "child pornography" on the ground that it fails to capture the abusive nature of the content.[18] In *Just Rights for Children Alliance v. S. Harish*, the Supreme Court of India similarly recognised that such material constitutes evidence of sexual abuse and exploitation rather than pornography. The Court recommended that Parliament substitute the expression "child sexual exploitative and abuse material" for "child pornography" throughout the POCSO Act, and directed that the former expression be used in judicial orders and judgments.[19] The adoption of this terminology reflects a broader shift towards a child-centred understanding of harm and victimisation.

AI-generated CSAEM generally falls into two categories. The first consists of fully synthetic depictions, where artificial intelligence systems generate realistic images or videos of children who do not exist in reality.[20] The second involves AI-manipulated content, where photographs or videos of real children are altered through deepfake technologies, face-swapping tools, or image-generation systems to create sexually explicit material.[21] Closely related are "nudification" applications that use AI to generate fabricated nude images from ordinary photographs, often without the knowledge or consent of the person depicted.[22] Beyond visual content, advances in conversational AI have also enabled chatbot-based sexual role-play systems and other forms of synthetic grooming that contribute to wider ecosystems of online child exploitation.[23]

---

[16] Garg and Shukla, *supra* note 3.
[17] Kokolaki and Fragopoulou, *supra* note 4.
[18] UNICEF, *supra* note 2.
[19] *Just Rights for Children Alliance*, *supra* note 13.
[20] Konstantinos Kosmas Gaitis, Chrystala Fakonti, Zoe Lonard *et al.*, *Legal Challenges in Tackling AI-Generated CSAM Across the UK, USA, Canada, Australia and New Zealand: Who Is Accountable According to the Law?* , in SEARCHLIGHT 2025: WHO BENEFITS? SHINING A LIGHT ON THE BUSINESS OF CHILD SEXUAL EXPLOITATION AND ABUSE 50 (Childlight, 2025).
[21] Subham Krishna Borah, Sheila Ramaswamy and Shekhar Seshadri, *The Online Specter: Artificial Intelligence and Its Risks for Child Sexual Abuse and Exploitation*, 21(2) JOURNAL OF INDIAN ASSOCIATION FOR CHILD AND ADOLESCENT MENTAL HEALTH 107 (2025).
[22] INTERNET WATCH FOUNDATION, *supra* note 1.
[23] INTERNET WATCH FOUNDATION, *supra* note 1.

 [ISSN 2581-5369]

The scale of this material has grown rapidly. In 2025 the Internet Watch Foundation assessed 8,029 AI-generated images and videos of child sexual abuse, a fourteen per cent increase on the previous year. The growth in video content was far sharper: the Foundation identified 3,443 AI-generated videos in 2025, against thirteen in 2024, and categorised sixty-five per cent of them within its most serious classification.[24] Alongside these figures, online communities dedicated to sharing AI-generated abuse material have continued to grow. AI-generated CSAEM is therefore no longer a speculative concern but an established feature of contemporary online exploitation.

AI-generated CSAEM differs from traditional abuse material in important respects. Conventional CSAEM generally serves as a record of a specific act of abuse involving an identifiable child victim. By contrast, AI-generated content may involve synthetic children, manipulated images of real children, or material created without any direct physical abuse during its production.[25] Yet the absence of physical contact does not necessarily eliminate harm. AI-generated CSAEM may facilitate grooming and sextortion, contribute to the re-victimisation of survivors, and reinforce and normalise sexual interest in children.

III. Child Rights Implications of AI-Generated CSAEM

A. International Child Rights Framework

The regulation of AI-generated CSAEM cannot be understood solely through the lens of criminal law. The United Nations Convention on the Rights of the Child requires States to adopt measures that protect children from abuse, exploitation, and harmful practices while ensuring their dignity, privacy, development, and wellbeing.[26] These obligations also include preventive measures.

Several provisions of the Convention are particularly relevant in the context of AI-generated CSAEM. Article 3 requires that the best interests of the child be treated as a primary consideration in all actions concerning children.[27] Article 16 protects children against arbitrary interference with their privacy, honour, and reputation.[28] Articles 19 and 34 require States to protect children from all forms of abuse and sexual exploitation, while Article 36 provides broader protection against any form of exploitation prejudicial to a child's welfare.[29] Article 39

[24] INTERNET WATCH FOUNDATION, *supra* note 1.
[25] Ó Ciardha, Buckley and Portnoff, *supra* note 6.
[26] The United Nations Convention on the Rights of the Child, 1989.
[27] The United Nations Convention on the Rights of the Child, 1989, art. 3.
[28] The United Nations Convention on the Rights of the Child, 1989, art. 16.
[29] The United Nations Convention on the Rights of the Child, 1989, arts. 19, 34 and 36.

 [ISSN 2581-5369]

further recognises the need for recovery and reintegration measures for child victims of exploitation and abuse.[30]

General Comment No. 25 on children's rights in relation to the digital environment emphasises that States must ensure that technological developments do not undermine children's rights, and must adopt measures to address digital forms of exploitation, abuse, and harm.[31] The question is therefore not merely whether AI-generated CSAEM fits within existing criminal offences, but whether legal and regulatory frameworks adequately safeguard children's rights in increasingly technology-mediated environments.

B. Synthetic Victimisation and the Limits of Traditional Victimhood

One of the most significant challenges posed by AI-generated CSAEM is its disruption of traditional understandings of victimhood. Conventional child-protection frameworks generally assume the existence of an identifiable child who has been directly abused during the production of exploitative material. Generative AI complicates this assumption by enabling the creation of sexualised depictions of children without direct physical abuse at the point of production.[32]

The absence of physical contact does not, however, mean the absence of harm. Children may become victims when their photographs are manipulated into sexually explicit content through deepfake technologies or nudification applications.[33] UNICEF has observed that AI systems have created circumstances in which children can be sexually exploited without their knowledge or participation, thereby expanding the traditional boundaries of victimisation.[34]

C. The Harms of AI-Generated CSAEM

Recent scholarship has challenged the claim that AI-generated CSAEM constitutes a victimless offence. Ó Ciardha, Buckley, and Portnoff identify several distinct harms associated with AI-generated abuse material that extend beyond the circumstances of its creation.[35]

AI-generated CSAEM can directly victimise children through deepfake technologies that transform ordinary photographs into sexually explicit content.[36] It may also contribute to the re-victimisation of existing survivors, where previously abused children are recreated or manipulated into new exploitative material.[37] Synthetic imagery may in addition facilitate

[30] The United Nations Convention on the Rights of the Child, 1989, art. 39.
[31] COMMITTEE ON THE RIGHTS OF THE CHILD, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, UN Doc. CRC/C/GC/25 (March 2, 2021).
[32] Kokolaki and Fragopoulou, *supra* note 4.
[33] Kokolaki and Fragopoulou, *supra* note 4.
[34] UNICEF, *supra* note 2.
[35] Ó Ciardha, Buckley and Portnoff, *supra* note 6.
[36] UNICEF, *supra* note 2.
[37] Ó Ciardha, Buckley and Portnoff, *supra* note 6.

 [ISSN 2581-5369]

grooming, coercion, sextortion, and other forms of technology-assisted exploitation by providing offenders with tools to manipulate or intimidate victims.[38]

Beyond these direct harms, researchers have expressed concern regarding the normalisation of child sexual exploitation and the reinforcement of deviant interests through repeated exposure to AI-generated abuse imagery.[39] While the relationship between synthetic content and contact offending remains contested, child-protection organisations have warned that such material may contribute to the normalisation of exploitative attitudes and behaviours.[40] AI-generated CSAEM has also facilitated peer-to-peer abuse among young people, including the creation of fabricated nude images of classmates and other forms of image-based sexual abuse occurring within educational settings.[41]

The harms are not confined to victims alone. The increasing volume of AI-generated content has created substantial challenges for law-enforcement agencies attempting to distinguish authentic abuse material from synthetic imagery.[42] This diverts investigative and victim-identification resources, and places additional burdens on agencies already struggling to address online exploitation.

D. From Victim-Based Protection to Harm-Based Protection

AI technologies have made it possible to create exploitative content in ways that do not fit neatly within earlier understandings of abuse. Focusing solely on whether a child was physically involved in the creation of an image therefore risks ignoring other forms of harm, including harm to privacy, dignity, reputation, and mental wellbeing.

A child-rights perspective requires a wider view of the problem.[43] The question should not be limited to whether a child was directly abused during the production of the material. It must also consider whether the content contributes to the exploitation, sexualisation, or victimisation of children, or undermines their rights and development.[44] Seen in this light, AI-generated CSAEM raises concerns that extend beyond conventional criminal law and calls for a more preventive and child-centred approach to regulation.

[38] Ó Ciardha, Buckley and Portnoff, *supra* note 6.
[39] INTERNET WATCH FOUNDATION, *supra* note 1.
[40] UNICEF, *supra* note 2.
[41] INTERNET WATCH FOUNDATION, *supra* note 1.
[42] INTERNET WATCH FOUNDATION, *supra* note 1.
[43] Garg and Shukla, *supra* note 3.
[44] Garg and Shukla, *supra* note 3.

 [ISSN 2581-5369]

IV. India's Existing Child Protection Framework

A. Constitutional and Statutory Foundations

The protection of children from sexual exploitation can be derived from constitutional principles and statutory safeguards. Article 21 of the Constitution guarantees the right to life and personal liberty, which has been judicially interpreted to include the rights to dignity, privacy, and protection from exploitation.[45] Article 15(3) empowers the State to make special provisions for children, while the Directive Principles of State Policy require the State to ensure that the tender age of children is not abused and that children are given opportunities to develop in conditions of freedom and dignity and are protected against exploitation.[46] Together, these provisions establish a constitutional foundation for child-protection measures in both physical and digital environments.

The principal statutory framework is provided by the Protection of Children from Sexual Offences Act, 2012 (POCSO). Sections 13 and 14 criminalise the use of a child for pornographic purposes, while Section 15, as substituted in 2019, penalises the storage or possession of child sexual abuse material, whether accompanied by a failure to delete, destroy, or report it, held for the purpose of transmitting, propagating, displaying, or distributing it, or held for a commercial purpose.[47] The definition inserted by the same amendment is the provision that matters most in the present context: it reaches any visual depiction of sexually explicit conduct involving a child, and expressly includes a digital or computer-generated image indistinguishable from an actual child, as well as an image created, adapted, or modified so as to appear to depict a child.[48] To that extent the Act is not confined to any particular method of production, and several commentators have argued that AI-generated CSAEM can, in many circumstances, be brought within its scope.[49]

Additional protection is provided by the Information Technology Act, 2000. Section 67B criminalises publishing or transmitting material depicting children in sexually explicit acts in electronic form, and separately criminalises creating text or digital images of such material and collecting, seeking, browsing, downloading, advertising, promoting, exchanging, or distributing it.[50]

---

[45] India Const. art. 21; *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[46] India Const. arts. 15(3), 39(e), 39(f) and 45.
[47] The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), ss. 13–15.
[48] The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), s. 2(1)(da), inserted by the Protection of Children from Sexual Offences (Amendment) Act, 2019 (Act 25 of 2019).
[49] Garg and Shukla, *supra* note 3.
[50] The Information Technology Act, 2000 (Act 21 of 2000), s. 67B.

 [ISSN 2581-5369]

B. Regulation of Online Child Sexual Exploitation

The increasing role of digital platforms in the dissemination of exploitative content has placed greater emphasis on intermediary regulation. Under Section 79 of the Information Technology Act, intermediaries may claim safe-harbour protection for third-party content, provided they comply with prescribed due-diligence obligations.[51] These obligations are supplemented by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which require intermediaries to inform users not to host material harmful to children, to remove unlawful content upon receiving valid notice, and, in the case of significant social media intermediaries, to deploy technical measures to identify child sexual abuse material proactively.[52]

That position has begun to change. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 introduced a definition of synthetically generated information and provided that the existing due-diligence obligations are to be read as extending to it.[53] The amended Rules further require intermediaries that offer computer resources capable of generating such information to deploy technical measures preventing users from producing material that contravenes the Information Technology Act, the Bharatiya Nyaya Sanhita, 2023, or the POCSO Act, and they name child sexual exploitative and abuse material expressly among the content to be prevented. They also impose labelling and provenance obligations on synthetically generated output.[54]

The framework therefore places significant responsibility on online platforms in preventing the circulation of child sexual abuse material, and the 2026 amendment extends part of that responsibility to the providers of generative tools. The primary statutes, however, were drafted before the widespread availability of generative AI systems and continue to say nothing about the responsibilities of AI developers and model providers. Such obligations as now exist rest on subordinate legislation rather than on any statutory recognition of synthetic victimisation.[55]

C. Institutional and Enforcement Mechanisms

India has also developed a number of institutional mechanisms to combat online child exploitation. The Indian Cyber Crime Coordination Centre (I4C) functions as a specialised body

[51] The Information Technology Act, 2000 (Act 21 of 2000), s. 79.
[52] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (February 25, 2021), rr. 3(1)(b), 3(1)(d) and 4(4).
[53] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (February 10, 2026), inserting rr. 2(1)(wa) and 2(1A).
[54] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, *supra* note 53, r. 3(3).
[55] Garg and Shukla, *supra* note 3.

 [ISSN 2581-5369]

for cybercrime prevention and investigation.[56] The National Cyber Crime Reporting Portal enables citizens to report cyber offences, including child sexual exploitation cases, while the Cyber Crime Prevention against Women and Children (CCPWC) scheme focuses on strengthening investigative capacity and victim protection.[57] More recently, the Sahyog Portal has sought to improve cooperation between intermediaries and government agencies by automating the issue of notices for the removal of, or disabling of access to, unlawful online content.[58]

These mechanisms demonstrate increasing recognition of online child exploitation as a significant policy concern. Nevertheless, the growing use of AI-generated content has created new enforcement challenges that existing institutions were not originally designed to address.

D. Judicial Developments

Judicial intervention has played an important role in shaping India's response to online child sexual exploitation. Early cases such as *Avnish Bajaj v. State (NCT of Delhi)*[59] raised questions regarding intermediary liability for the online dissemination of sexually explicit content.[60] Later proceedings pressed for stronger measures to identify, report, and remove child sexual abuse material from online platforms: *Kamlesh Vaswani v. Union of India* produced a series of interim directions on the blocking of websites hosting such material,[61] while the *suo motu* proceedings registered on the Prajwala letter led to the constitution of an expert committee and to standard operating procedures for the detection, reporting, and removal of such material.[62]

The most significant recent development is the Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish*.[63] The Court discouraged the expression "child pornography" and endorsed the use of the term child sexual exploitative and abuse material, recognising that such content constitutes evidence of abuse and exploitation rather than consensual sexual expression. It further held that Section 15 of the POCSO Act creates three distinct offences and that

[56] MINISTRY OF HOME AFFAIRS, Government of India, Indian Cyber Crime Coordination Centre (I4C).
[57] MINISTRY OF HOME AFFAIRS, Government of India, National Cyber Crime Reporting Portal; MINISTRY OF HOME AFFAIRS, Government of India, Cyber Crime Prevention against Women and Children (CCPWC) Scheme.
[58] MINISTRY OF HOME AFFAIRS, Government of India, Sahyog Portal (Indian Cyber Crime Coordination Centre, operational from October 2024); see also Garg and Shukla, *supra* note 3.
[59] *Avnish Bajaj v. State (NCT of Delhi)*, 2008 SCC OnLine Del 688 (Delhi High Ct., May 29, 2008).
[60] *Avnish Bajaj*, *supra* note 59. The High Court declined to discharge the managing director of the intermediary in respect of the offence under s. 67 read with s. 85 of the Information Technology Act, 2000.
[61] *Kamlesh Vaswani v. Union of India*, W.P. (Civil) No. 177 of 2013 (Sup. Ct. India).
[62] *In re Prajwala Letter dated 18.2.2015 Videos of Sexual Violence and Recommendations*, Suo Motu Writ Petition (Crl.) No. 3 of 2015 (Sup. Ct. India, disposed of Aug. 1, 2023).
[63] *Just Rights for Children Alliance*, *supra* note 13.

 [ISSN 2581-5369]

possession may be constructive, so that a person who exercises control over such material and fails to delete, destroy, or report it may incur liability.[64]

Taken together, these constitutional provisions, statutory frameworks, institutional mechanisms, and judicial developments suggest that India possesses a relatively comprehensive legal architecture for addressing child sexual exploitation. The critical question, however, is whether a framework developed primarily for traditional forms of abuse remains adequate in responding to the distinctive challenges posed by generative AI.

V. Evaluating the Adequacy of India's Framework in the Generative AI Era

A. Existing Strengths of the Framework

Any assessment of India's response to AI-generated CSAEM must begin by recognising the strengths of the existing framework.

The relevant statutory provisions are, in important respects, indifferent to the technology used. Neither the definition of child sexual abuse material in the POCSO Act nor Section 67B of the Information Technology Act confines liability to material produced by conventional techniques.[65,66] The focus of these provisions is on the exploitative character of the material rather than on the technology used to create it. This enables existing offences to be applied to many forms of AI-generated content, particularly where real children are depicted or where sexually explicit material is created using photographs of actual minors.[67]

Judicial developments have also adopted expansive interpretations of child-protection legislation. In *Just Rights for Children Alliance v. S. Harish*,[68] the Supreme Court emphasised a child-centred approach to online sexual exploitation and rejected narrow understandings of child sexual abuse material.[69] Such interpretive flexibility increases the likelihood that courts will extend existing protections to emerging forms of AI-enabled exploitation.

Finally, India has developed a growing institutional infrastructure for combating online child exploitation through mechanisms such as the Indian Cyber Crime Coordination Centre, the National Cyber Crime Reporting Portal, the CCPWC scheme, and the Sahyog Portal.[70] While

[64] *Just Rights for Children Alliance*, *supra* note 13.
[65] The Protection of Children from Sexual Offences Act, 2012, *supra* note 47.
[66] The Information Technology Act, 2000, s. 67B, *supra* note 50.
[67] Garg and Shukla, *supra* note 3.
[68] *Just Rights for Children Alliance*, *supra* note 13.
[69] *Just Rights for Children Alliance*, *supra* note 13.
[70] Yadav, *supra* note 15.

 [ISSN 2581-5369]

these institutions were not specifically created to address generative AI, they provide an important foundation upon which future regulatory responses can be built.

The existence of these provisions does not, however, establish their sufficiency. Generative AI has created several challenges that limit the capacity of this framework to address new forms of abuse.

B. The Synthetic Child Problem

One of the most difficult questions raised by AI-generated CSAEM concerns content depicting children who do not exist in reality. Traditional child-protection laws generally assume the presence of an identifiable child victim who has been abused, exploited, or otherwise harmed in the creation of the material.[71] AI-generated imagery challenges this assumption by making it possible to create realistic sexualised depictions of entirely fictional children.

This creates an ambiguity within existing legal frameworks. The definitional language of the POCSO Act is capable of reaching computer-generated images indistinguishable from an actual child, but Sections 13 and 14 are framed around the use of a child, and Section 67B of the Information Technology Act[72] was enacted at a time when such material could not be created without reference to a real child.[73] Uncertainty therefore remains as to whether, and by which route, fully AI-generated depictions fall within the intended scope of these provisions.

Comparative research shows that this challenge is not limited to India. Several jurisdictions, including the United States, Canada, Australia, and New Zealand, continue to grapple with the legal status of AI-generated content depicting fictional children.[74] The difficulty arises because criminalisation in these frameworks is generally justified by the need to protect an identifiable victim. Where no such victim exists, courts and legislators must determine whether the content should nevertheless be prohibited because of its broader contribution to child sexual exploitation.

A narrow interpretation may create significant enforcement gaps, since excluding synthetic content risks normalising child sexual exploitation.[75] The question therefore exposes a broader tension between traditional victim-based models of protection and emerging harm-based approaches.

[71] Ó Ciardha, Buckley and Portnoff, *supra* note 6.
[72] The Information Technology Act, 2000, s. 67B, *supra* note 50.
[73] Garg and Shukla, *supra* note 3.
[74] Gaitis, Fakonti, Lonard *et al.*, *supra* note 20.
[75] Kokolaki and Fragopoulou, *supra* note 4.

 [ISSN 2581-5369]

C. Deepfake Victimisation and Image-Based Sexual Abuse

While debates concerning fictional children remain important, the most immediate threat posed by generative AI arises from the manipulation of images of real children. Deepfake technologies and nudification applications have made it possible to transform ordinary photographs into sexually explicit content without the knowledge or consent of the child concerned.[76]

A child whose image is manipulated into explicit content may suffer reputational damage, emotional distress, social stigma, and long-term psychological harm despite never having participated in the creation of the material.[77] Recent studies have highlighted the increasing use of AI-generated sexual imagery in cases involving bullying, sextortion, coercion, and peer-to-peer abuse among young people.[78]

Although existing legal provisions may be capable of addressing some instances of deepfake abuse, they do not expressly recognise synthetic victimisation as a distinct form of harm. This creates uncertainty regarding the scope of protection available to children whose images are digitally manipulated rather than conventionally recorded.

VI. Towards a Child-Centred AI Governance Framework

The challenges posed by AI-generated CSAEM cannot be addressed through criminal law alone. While existing statutory provisions provide a useful starting point, the analysis undertaken in this paper demonstrates the need for a broader child-centred governance framework capable of responding to the realities of generative AI.

At the legislative level, greater clarity is required regarding the legal status of AI-generated CSAEM. Express statutory recognition of synthetic abuse material, including fully AI-generated child depictions and deepfake sexual imagery involving real children, would reduce interpretive uncertainty and strengthen enforcement efforts.[79] Such reforms would also align domestic law with emerging international concerns regarding synthetic victimisation and technology-enabled exploitation.[80]

Regulatory responses must move beyond *post facto* enforcement and place greater emphasis on prevention. AI developers and platform operators should be required to adopt safety-by-design measures, conduct risk assessments for systems capable of generating visual content, and implement safeguards aimed at preventing the creation and dissemination of exploitative

[76] UNICEF, *supra* note 2.
[77] Ó Ciardha, Buckley and Portnoff, *supra* note 6.
[78] UNICEF, *supra* note 2.
[79] UNICEF, *supra* note 2.
[80] Gaitis, Fakonti, Lonard *et al.*, *supra* note 20.

 [ISSN 2581-5369]

material.[81] The 2026 amendment to the Intermediary Guidelines makes a beginning in this direction, but its obligations are framed around the prevention of generation and the labelling of output rather than around a broader duty of care owed to children, and they carry the vulnerabilities of subordinate legislation.[82]

Platform governance also requires closer attention. Intermediaries and AI service providers should be subject to clear reporting, transparency, and content-moderation obligations, particularly where their services may be misused to generate CSAEM.[83] At the same time, law-enforcement agencies must be equipped with the specialised technological expertise and forensic capabilities necessary to investigate AI-enabled offences effectively. Given the transnational nature of online exploitation, international cooperation will remain essential for identifying offenders, removing harmful content, and sharing investigative resources.

Finally, a child-rights approach requires greater emphasis on prevention, awareness, and support. Digital literacy initiatives, age-appropriate online safety education, and accessible support mechanisms for victims of image-based sexual abuse should form part of any long-term strategy for protecting children in digital environments.[84] As generative AI continues to evolve, child-protection frameworks must evolve alongside it, ensuring that technological innovation does not come at the expense of children's rights, dignity, and safety.

VII. Conclusion

The rapid growth of generative artificial intelligence has created new challenges for child protection that existing legal frameworks were never designed to address. AI-generated child sexual abuse and exploitation material has blurred the line between real and synthetic content, making it easier to create, manipulate, and circulate exploitative material. These developments have raised difficult legal questions about victimhood, accountability, and the scope of existing child-protection laws.

This paper has shown that India is not without legal safeguards to deal with these emerging challenges. The definitional breadth of the Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000, together with the Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish*, provides a reasonably strong legal foundation for addressing several forms of AI-generated CSAEM. In many situations, these provisions are

[81] Kokolaki and Fragopoulou, *supra* note 4.
[82] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, *supra* note 53.
[83] UNICEF, *supra* note 2.
[84] Committee on the Rights of the Child, *supra* note 31.

 [ISSN 2581-5369]

capable of being interpreted broadly enough to cover technology-enabled forms of child sexual exploitation.

At the same time, the analysis demonstrates that the existing framework is not fully equipped to deal with the realities of generative AI. Questions surrounding fully synthetic child depictions, deepfake victimisation, the responsibilities of AI developers and digital platforms, and the difficulties of investigating AI-generated content continue to expose important legal and regulatory gaps. The framework remains largely reactive, addressing exploitation after it occurs rather than preventing it at the design and deployment stage of AI technologies.

Ultimately, AI-generated CSAEM should not be viewed only as a technological or criminal-law issue. It is, above all, a child-rights issue. Protecting children in the digital age requires more than expanding criminal liability; it calls for a legal framework that prioritises prevention, accountability, and the best interests of the child. As generative AI becomes more sophisticated and widely available, India's child-protection regime must continue to evolve so that technological innovation does not come at the cost of children's dignity, safety, and rights.

*****

 [ISSN 2581-5369]