The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CHILD SEXUAL ABUSE MATERIAL IN DIGITAL ERA: RETHINKING INDIA'S LEGAL RESPONSE.

VISHIKA DHALIA[1]

ABSTRACT

Child Sexual Abuse Material (CSAM) has evolved into a complex digital governance challenge driven by artificial intelligence, encryption, and transnational networks. This blog critically examines India's legal framework, identifies emerging regulatory gaps, and advocates a technology-responsive, victim-centric approach to strengthen child protection.

Keywords: Child Sexual Abuse Material (CSAM); Artificial Intelligence; transnational networks.

I. FROM "CHILD PORNOGRAPHY" TO CHILD SEXUAL ABUSE MATERIAL (CSAM)

The language used to describe the sexual offences committed against children is of great importance when it comes to legal measures. Historically, such sexual materials were known as 'child pornography' but this name has increasingly lost favour since it suggests consent related to adult pornography.[2] The international institutions, police forces and child rights organisations nowadays prefer CSAM (Child Sexual Abuse Material) or CSEAM (Child Sexual Exploitation and Abuse Material) because all the images or videos should be seen as proof of sexual abuse of the child and not consensual acts[3]

[1] A Third Year student (B.A.LL.B.) at National Law University, Jodhpur

[2] INTERPOL, Appropriate Terminology: Crimes Against Children, https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology (last visited Aug. 2, 2026).

[3] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), ECPAT Int'l, https://ecpat.org/luxembourg-guidelines/ (last visited Aug. 2, 2026).

The move to the new terms has important legal consequences. CSAM has become not obscene content, but continuing violation of children's rights because each download or distribution of the material continues the act of abuse.[4] Similarly, the current scholarly studies claim that the development of digital space has turned the issue of CSAM into a continuing form of exploitation which needs victim-based regulation and detection.[5]

India is gradually adopting this perspective. Judicial decisions, such as In Re: Prajwala,[6] and the modern policy discussion more frequently consider CSAM as continuing violation of children's rights due to the challenges of artificial intelligence and encrypted communications.

II. INDIA'S CURRENT LEGAL FRAMEWORK: A LAYERED APPROACH TOWARDS CSAM

India's response towards CSAM involves a combination of criminal laws, cyber laws, intermediary liability laws, and child protection laws. The key piece of legislation is the Protection of Children from Sexual Offences (POCSO) Act, 2012, which includes Sections 13 to 15,[7] which makes the production, dissemination, possession, transmission and commercialization of CSAM illegal, since its continued distribution leads to further abuse of children.

The Information Technology Act, 2000, with Section 67B[8] of it making the electronic communication, distribution, access, and publication of sexually explicit materials with children illegal supplements POCSO. The Bharatiya Nyaya Sanhita, 2023[9] strengthens criminal liability for technology-enabled offenses against children.

Besides criminalization, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,[10] 2021 puts obligations on intermediaries for due diligence, and

[4] Supra note 1.
[5] Dhruv Garg & Dedipyaman Shukla, Combatting AI-Generated Child Sexual Exploitation and Abuse Material: An Analysis of India's Techno-Legal Response, 21 Indian J. L. & Tech. (2025).
[6] In Re: Prajwala Letter Dated 18.02.2015 Videos of Sexual Violence and Recommendations, Suo Motu Writ Petition (Criminal) No. 3 of 2015.
[7] Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 13–15, Acts of Parliament, 2012.
[8] Information Technology Act, No. 21 of 2000, § 67B, Acts of Parliament, 2000.
[9] Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023.
[10] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, pt. II, sec. 3(i), Feb. 25, 2021.

recent changes in which require the elimination of CSAM, including that created through artificial intelligence within two hours show the focus on timely action. Digital Personal Data Protection Act, 2023[11] ensures data protection of children.

From institutional perspective, the NCPCR,[12] I4C,[13] SAHYOG Portal,[14] and Fast Track Special POCSO Courts[15] enhance reporting, investigation and victim protection. All these efforts create a strong legal framework, but which requires adaptation in light of developing technologies.

III. EMERGING CHALLENGES IN THE DIGITAL ERA: EXAMINING THE LIMITS OF THE INDIAN LEGAL REGIME

Although there is an extensive Indian legal regime, the rate of technology innovation has always outstripped the enforcement capabilities, revealing major deficiencies in regulation and investigations. The problem is not the lack of prohibition on certain activities but the inability of the legal regime to react to the fast-changing forms of online child sexual exploitation.[16]

Artificial Intelligence (AI)-Generated CSAM. The advent of generative AI is creating a new legal vacuum as it enables the creation of realistic AI-created CSAM, deepfakes, and manipulation, which is then used for grooming, re-victimization, and normalization of exploitative behavior. The Indian legal regime, including POCSO Act, 2012, and section 67B of the Information Technology Act, 2000, were designed mainly to deal with the reality-based images of the abuse. There is no clear provision in these acts concerning the generated CSAM.

[11] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023.
[12] National Commission for Protection of Child Rights, Being Safe Online: Cyber Safety Guidelines for Children, https://ncpcr.gov.in (last visited Aug. 2, 2026).
[13] Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India, https://www.cybercrime.gov.in (last visited Aug. 2, 2026).
[14] Ministry of Home Affairs, SAHYOG Portal for Reporting Child Sexual Exploitation Material, https://www.cybercrime.gov.in (last visited Aug. 2, 2026).
[15] Department of Justice, Government of India, Scheme for Fast Track Special Courts (FTSCs) Including Exclusive POCSO Courts, https://doj.gov.in (last visited Aug. 2, 2026).
[16] Vipul Kumar et al., Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation, Comput. & Sec. (Elsevier 2025).

This creates uncertainty regarding criminal liability, intermediary obligations, and evidentiary standards in cases involving synthetic exploitation[17]

Cross-Border Investigation. The borderless character of online mediums adds to the complexity of enforcement mechanisms. CSAM is often stored in cloud storage located abroad and distributed via encrypted applications and dark web. As such, cross-border investigations depend significantly on Mutual Legal Assistance Treaties (MLATs), cooperation with the platform and international police organizations. Often, procedural challenges and fragmentation of digital evidence hinder the prosecution process, making it necessary to foster better coordination and uniform digital evidence procedures.[18]

Privacy versus Regulation. With increased use of end-to-end encryption technologies, the balance between privacy and child protection has become particularly challenging. On one hand, encryption protects privacy of the lawful user. At the same time, it hinders detection, tracing and removal of CSAM by intermediaries and investigative agencies. Thus, the key to successful regulation is to enhance intermediary responsibility and capability to investigate CSAM without undermining the right to privacy enshrined in the constitution.

IV. RETHINKING INDIA'S LEGAL RESPONSE

The Indian legal approach to addressing CSAM needs to go beyond being largely repressive and develop into a technology-savvy form of digital governance. Whereas the POCSO Act, 2012, the Information Technology Act, 2000, and intermediaries' regulations create a robust statutory basis, technological advancement has identified loopholes in the existing laws which the criminal laws alone are unable to fill. Future legislative changes in the area would need to include explicit regulation of AI-generated CSAM and greater intermediary liability in automated CSAM detection and preservation of digital evidence.

Another key step to consider would be the strengthening of the cross-border enforcement of CSAM-related legislation through the establishment of rapid digital evidence sharing systems, increased collaboration with INTERPOL, INHOPE, and WeProtect Global Alliance, and

[17] AI-Generated Child Sexual Abuse Material: Emerging Regulatory Challenges, Computer L. & Sec. Rev. (2025).
[18] WeProtect Global Alliance, Global Threat Assessment 2023: Working Together to End Child Sexual Exploitation and Abuse Online (2023), https://www.weprotect.org

development of specialized cyber-forensic techniques. However, all these initiatives have to be conducted consistently with constitutional guarantees on the right to privacy of individuals and make sure that child protection is achieved through proportional and accountable regulation and not through arbitrary surveillance of children's digital lives.

V. CONCLUSION

The digital environment has revolutionized the way child sexual exploitation takes place, making traditional legal responses less relevant. Despite India having a comprehensive legislative regime for tackling CSAM, modern technology like artificial intelligence, encryption of data, and borderless digital environment poses serious challenges for the implementation of such legislation. While addressing this problem calls for not only the strengthening of laws but also adaptive governance to keep up with innovation and international cooperation, among other considerations, a forward-looking legislative regime will be one which evolves along with technology to enable it to accomplish its primary purpose of ensuring the safety of children in the digital world.