CIRCULATION OF ONLINE CHILD SEXUAL ABUSE MATERIAL AND CHILD PROTECTION: GAPS IN INDIAN LAW

Divya Mishra*

ABSTRACT

The circulation of online child sexual abuse material (CSAM) has emerged as a serious threat against children in cyberspace. It constitutes a form of continuous harm that is intensified by transmission amid rapid digital advancements. CSAM serves as evidence of abuse against children and results in the re-victimisation of the child through its transmission on digital platforms. Although Indian law criminalises the production, storage, possession and transmission of CSAM, it largely fails to recognise the continuous nature of harm arising from its circulation. This article will examine the gaps and challenges within the existing legal frameworks that undermine effective prevention and child protection in the digital space. It analyses statutory provisions under the Information Technology Act and the POCSO Act, along with regulatory mechanisms, intermediary obligations and enforcement challenges. For this purpose, a doctrinal research methodology is adopted, utilising both primary and secondary sources of legal research. The objective of this article is to examine the adequacy of the Indian legal framework in addressing the circulation of online child sexual abuse material from a child protection perspective. It further highlights the necessity of robust regulatory mechanisms, effective implementation and greater emphasis on prevention and victim rehabilitation.

Keywords: Child Sexual Abuse Material (CSAM), Circulation of CSAM, Child Protection, Indian Legal Framework.

INTRODUCTION

Information and communication technology has become an essential requirement in the modern era. Technological developments in digital platforms have enabled individuals to

*LLM, FIRST YEAR, HIMACHAL PRADESH UNIVERSITY SUMMER HILL, SHIMLA.

connect across geographical boundaries within seconds. Children have also adopted this digital culture, which has expanded significantly after the COVID-19 lockdown.[1] The exposure of children to digital media platforms, particularly social media and gaming platforms, has heightened the vulnerability of children in cyberspace. India has also been affected by this crime against children. According to the NCRB Report 2022,[2] there was 32% rise in cybercrime against children, with offences relating to Child Sexual Abuse Material (CSAM) among the more severe crimes against minors, and this trend further intensified in 2023[3] report.

Several laws protect children in the digital space, including the Information Technology (IT) Act, 2000, Protection of Children from Sexual Offences (POCSO) Act, 2012, Bharatiya Nyaya Sanhita (BNS), 2023, and the Digital Personal Data Protection (DPDP) Act, 2023. However, CSAM is specifically addressed under the IT Act and POCSO Act under the heading of child pornography. Although the transmission is criminalised under the Act, effective control over its circulation remains limited, which adversely affects child protection and rehabilitation. This article will examine the problem of the circulation of CSAM and the gaps in India's legal framework that undermine effective child protection. The main aim of this article is to underscore the harms arising from the circulation of CSAM and to ensure the protection of children in digital spaces.

CONCEPTUAL UNDERSTANDING OF CSAM & CHILD PROTECTION CONCERNS

Earlier, the term 'Child Pornography' was used in various national and international legislations to describe visual depictions of children engaged in sexually explicit activities. Nowadays, the term 'child sexual abuse material' is preferred to 'child pornography'. This is because the term pornography is generally associated with consensual sexual expression and distribution. In the context of children, consent is legally meaningless. Accordingly, any material depicting such acts is considered sexual abuse. The term 'child pornography' undermines the seriousness of sexual abuse and fails to adequately represent the interests of

[1] Sadhna Singh, 'Online Safety for Children: Protecting the Next Generation from Harm' (NITI Aayog) https://niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf accessed 6 January 2026.
[2] National Crime Records Bureau, 'Crime in India 2022' (Government of India, Ministry of Home Affairs) https://www.ncrb.gov.in/crime-in-india-year-wise.html?year=2022&keyword= accessed 6 January 2026.
[3] National Crime Records Bureau, 'Crime in India 2023' (Government of India, Ministry of Home Affairs) https://www.ncrb.gov.in/crime-in-india-year-wise.html?year=2023&keyword= accessed 6 January 2026.

victims.[4] However, under Indian legislation, CSAM is not defined as a separate offence. As a result, the earlier terminology continues to be used interchangeably.

CSAM indicates that children have been subjected to sexual abuse, which may occur through grooming, coercion or other forms of sexual exploitation. It contains audio, visual or written material, including digitally generated content, depicting sexual abuse of children.

Digital platforms, including social media, the dark web, and other online websites, play a crucial role in the production and distribution of such material. Such platforms enable the transmission of these materials across the world with a single click. This significantly complicates both the detection and prevention of its transmission.

In this regard, the National Human Rights Commission (NHRC) issued an advisory for the protection of the rights of children against the production, distribution and consumption of CSAM. According to the advisory, the production of CSAM creates a permanent record of child sexual abuse, while its transmission results in perpetual victimisation.[5] It serves as proof of humiliation and intrusion into the privacy of children, thereby undermining their dignity. A survey conducted by a Canadian Child Protection Organisation found that CSAM survivors experienced the distribution impacts them differently from the initial abuse. They continue to suffer due to the permanent nature of such material and its ongoing circulation.[6]

Once an image is uploaded online, it may be removed from a platform, but it cannot be destroyed. For this reason, abusers frequently use CSAM for revictimisation and to stalk children. Even after the original producer is identified, such material continues to be used to groom other children for future abuse. This continuous threat and prolonged online exposure adversely affect children's psychological well-being and further disrupt their overall development.

[4] INTERPOL, 'Appropriate Terminology' https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology#:~:text=In%20fact%2C%20we%20want%20you,words%20such%20as%20%22porn%22. Accessed 7 January 2026.

[5] National Human Rights Commission, 'Advisory for Protection of the Rights of Children against Production, Distribution and Consumption of Child Sexual Abuse Material (CSAM)' (New Delhi, 27 October 2023) https://nhrc.nic.in/assets/uploads/other_advisories/1721815751_9a25ee261378deda78f2.pdf accessed 8 January 2026.

[6] Canadian Centre for Child Protection, 'SURVIVORS' SURVEY EXECUTIVE SUMMARY 2017' C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf accessed 9 January 2026.

LEGAL FRAMEWORK GOVERNING CSAM IN INDIA

In Indian legislation, CSAM is specifically dealt with under the Information Technology Act (IT), 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, both criminalize the production, storage and transmission of such material. The Bhartiya Nyaya Sanhita (BNS) supplement these provisions by addressing obscene material. While the DPDP Act does not expressly regulate CSAM, it indirectly strengthens child protection in the digital ecosystem. An analysis of these provisions enables an assessment of the adequacy of the legislative framework in addressing the circulation of CSAM. However, the extent to which these statutes effectively address the distinct and continuing harm caused by the circulation of CSAM remains a critical issue.

Information and Technology Act, 2000: The Information Technology Act, 2000, is the primary legislation dealing with the digital environment and computer-related crimes. To address obscene material in the digital domain, the Act initially contained only Section 67.[7] This provision broadly covers obscene material without making any specific distinction. Subsequently, the Information Technology (Amendment) Act, 2008, was enacted, through which Sections 67A and 67B were inserted to address specific forms of sexually explicit content.

Section 67B is the most relevant provision as it specifically addresses the publication and transmission of sexually explicit material depicting children.[8] Although Sections 67 and 67A[9] deal with obscene material, they do not distinguish between adults and children. Sexually explicit material involving children is not merely content; it constitutes evidence of abuse. It is a more serious and sensitive matter than other sexually explicit material. Therefore, it requires a separate and stricter provision.

Section 67B broadly criminalises the production, publication, searching, storage and distribution of obscene and indecent material depicting children. It demonstrates that not only active participation in the production of CSAM constitutes an offence but that its search, storage and distribution are also punishable.[10] Moreover, distribution makes such material

[7] Information Technology Act 2000 s.67
[8] Ibid s.67B
[9] Ibid s.67A
[10] Rahul Kailash Bharti, 'Offences Related to Obscenity, Child Pornography, and Online Harassment (Sections 67, 67A, 67B of the IT Act, 2000)' (24 July 2025) https://doi.org/10.70593/978-93-7185-183-1 available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5388650 accessed 10 January 2026.

accessible to others, rendering it an unending phenomenon with global availability. This reflects the seriousness of the offence, which is further aggravated by repeated circulation through digital platforms.

In addition to these provisions, Section 2(w) of the Act defines an 'intermediary' as any person who, on behalf of another, receives, stores or transmits electronic records. Such intermediaries include telecom service providers, internet service providers, search engines and other similar entities.[11] Section 79 of the Act grants intermediaries conditional exemption from liability, subject to the observance of due diligence and compliance with government-prescribed guidelines.[12] To implement this due diligence requirement, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose specific obligations on intermediaries, including the timely removal of unlawful content.[13] However, if intermediaries conspire in unlawful acts or fail to remove links or material relating to such acts, they cannot avail themselves of this exemption. In the context of CSAM, this conditional safe harbour can limit the accountability of intermediaries. This can reduce the compliance burden on intermediaries, which may inadvertently enable the continued circulation of such unlawful material in the absence of effective supervision. Despite criminalising CSAM and prescribing intermediary obligations, the IT Act does not fully account for the distinct vulnerability of children involved.

Protection of Children from Sexual Offences (POCSO) Act, 2012: To address gaps in the IPC and the IT Act, the POCSO Act was enacted to provide a child-specific and comprehensive framework against sexual abuse. The Act establishes a penal framework that criminalises various forms of CSAM-related offences. The POCSO Act is a child-centric legislation that defines child pornography under section 2(da). Under this provision, child pornography includes any visual depiction, such as photographs, videos or computer-generated images.[14] Section 13 of the Act criminalises the use of a child for pornographic purposes. The provision states that the use of a child in any media for sexual gratification constitutes an offence. Such use includes the depiction of sexual organs, engagement in sexual activity or obscene

[11] Information Technology Act 2000 (n 7) s.2(w)
[12] Ibid s.79
[13] Press Information Bureau, 'Government of India Taking Measures Against Online Pornography' (Delhi, 19 March 2025) https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2113098&reg=3&lang=2 accessed 10 January 2026.
[14] Protection of Children from Sexual Offences Act 2012 s.2(da)

representation for production, publication or transmission, constitutes the offence of using a child for pornographic purposes.[15]

Section 15 of the Act assumes particular significance in addressing the transmission of CSAM.[16] Section 15(1) of the Act specifically addresses the offence relating to the storage of pornographic material.[17] The provision penalises the storage or possession of child pornographic material where there is an intention to share or transmit such content. This reflects the legislative recognition that even passive involvement may contribute to the circulation of CSAM and therefore attract penal consequences.

Section 15(2) penalises the storage or possession of child pornographic material intended for transmission, propagation, display or distribution.[18] This provision is preventive in nature, as it seeks to curb harm at an early stage, before intent culminates in actual transmission. Once such material is transmitted, its circulation intensifies, and detection becomes increasingly difficult.

Section 15(3) provides that any person who uses such material for commercial purposes shall be liable to imprisonment for a term which may extend up to five years, along with a fine.[19] This provision targets profit-driven exploitation. Such exploitation poses heightened harm by enabling the large-scale availability of such content and incentivising its production.

Section 15 of the Act underscores transmission as a critical concern; however, it continues to conceptualise transmission as a discrete offence rather than as part of a continuing chain of circulation. As a result, the prevention and detection of such offences remain challenging, which limits the effective implementation of this provision in practice.

Bharatiya Nyaya Sanhita (BNS), 2023: The Bharatiya Nyaya Sanhita (BNS), 2023, functioned as a substantive law that provides punishment for various offences against society. Although it did not contain specific provisions addressing CSAM, it supplemented offences relating to CSAM under the IT and the POCSO Act. Sections 294 and 295 of this act deal with obscene material. Section 294 defines obscene material, including material in electronic form, and criminalises its production, sale, distribution and public exhibition of obscene content, both

[15] Ibid s.13
[16] Ibid s.15
[17] Ibid s.15(1)
[18] Ibid s.15(2)
[19] Ibid s.15(3)

in physical and electronic forms.[20] Section 295 further criminalises the sale, distribution or circulation of any obscene object to a child.[21] While these offences seek to regulate obscenity and its circulation, they fail to address child sexual abuse and the vulnerability of children in the digital environment.

Digital Personal Data Protection (DPDP) Act, 2023: This Act does not specifically address CSAM. However, it contributes to the protection of children in cyberspace by regulating the processing of children's personal data. Section 9 of the Act mandates parental consent for processing a child's data and prohibits the use of such data in a manner detrimental to the well-being of the child.[22]

GAPS AND CHALLENGES IN PROTECTING CHILDREN FROM CSAM CIRCULATION

Despite the existence of these legislative frameworks, the incidence of CSAM continues to rise in India, indicating the presence of gaps that undermine the effectiveness of the law. Evolving technology and its advanced features further pose challenges, thereby widening existing regulatory gaps and increasing threats to children.

One of the major gaps is that Indian legislation recognises the transmission of CSAM like other criminal offences and is treated as a discrete act. This approach overlooks the continuous nature of such harm, as once circulated in the digital environment, it becomes effectively permanent. Although the content may be removed from a particular platform, it cannot be fully eradicated from cyberspace, leading to repeated uploads and continued sharing across platforms. Each act of browsing, viewing, downloading or sharing constitutes renewed harm and further undermines the dignity of the child.

This reveals another significant gap in the Indian legal framework, which remains predominantly punitive rather than preventive in its approach. While the law focuses on punishing offenders after the commission of the offence, it pays limited attention to preventing further circulation, thereby allowing such material to persist on digital platforms.

[20] Bharatiya Nyaya Sanhita 2023 s.294
[21] Ibid s.295
[22] The Digital Personal Data Protection Act 2023, s.9

In addressing CSAM on digital platforms, intermediaries play a crucial role. They are required to exercise due diligence, including reporting and the timely removal of unlawful content. However, the implementation of these obligations reveals significant gaps in practice. Intermediaries frequently fail to proactively report or remove CSAM from their platforms, thereby facilitating its continued circulation. The conditional safe harbour protection under Section 79 further limits intermediary accountability, often providing an avenue to evade responsibility unless explicit non-compliance is established.

In this regard, the Ministry of Electronics and Information Technology (MeitY) has issued notices to platforms such as X, YouTube and Telegram, warning that failure to comply will result in the withdrawal of safe regulatory interventions.[23]

The complex and evolving nature of digital technology further challenges the existing legal framework and widens the gaps in addressing the circulation of CSAM. Technological advancements that enable anonymity on digital platforms, including the use of avatars in place of real identities, significantly hinder detection and identification efforts. End-to-end encryption further complicates monitoring and enforcement mechanisms, thereby increasing risks to children.

In India, the circulation of CSAM witnessed a significant increase during the lockdown and has continued to rise thereafter. In 2021, the Central Bureau of Investigation (CBI) launched 'Operation Carbon' targeting the uploading, circulation, sale and viewing of CSAM through social media platforms and groups.[24] In 2022, based on information received from Interpol Singapore, CBI launched another operation named 'Megha Chakra'. Under this operation, the CBI carried out searches across 21 states relating to the circulation, downloading and sharing of CSAM using cloud storage.[25] Despite these enforcement efforts, a covert operation conducted by a Hyderabad-based NGO in 2023 indicated that CSAM was being openly

[23] Press Information Bureau, 'MEITY cracks down on intermediaries over Child Sexual Abuse Material, sends notices to X, Youtube & Telegram (Delhi, 06 October 2023) https://www.pib.gov.in/PressReleaseframePage.aspx? PRID=1965078&reg=3&lang=2 accessed 12 January 2026.

[24] Devesh K. Pandey, 'Operation Megh Chakra: 50 under CBI scanner over child pornography' (New Delhi, 25 September 22) https://www.thehindu.com/news/national/sharing-of-child-sexual-abuse-material-cbi-raids-56-places-in-19-states-and-1-ut/article65930142.ece/amp accessed 13 January 2026.

[25] Central Bureau of Investigation, 'CBI today conducts national wide searches in meticulous operation in Megh Chakra at around 59 locations in 21 states/UT etc in two cases related to download/ circulation of CSAM' (24 September 2022) https://cbi.gov.in/press-detail/NTI2Ng accessed 13 January 2026.

circulated on Telegram.[26] These highlight how difficult it is to prevent the online circulation of CSAM.

Certain social factors also play an important role in facilitating the circulation of CSAM on digital platforms. Limited digital literacy among users contributes to the misuse of online platforms, as many individuals lack adequate awareness of the digital environment they engage with and remain unaware of safe and responsible online practices. As a result, users may unintentionally engage with or share harmful content, thereby contributing to the continued circulation of CSAM.

The lack of sex education further aggravates this problem. In India, sex education is often treated as a sensitive and private subject and is not discussed openly. This limited awareness may lead individuals, particularly children, to seek information online without understanding the associated risks, which increases exposure to sexually exploitative material and facilitates its circulation.

Underreporting is another significant challenge. Due to feelings of shame, guilt and lack of awareness, victims and their families often hesitate to report incidents of online sexual exploitation. Such delays hinder timely investigation and removal of such content, allowing CSAM to remain accessible on digital platforms for longer periods.

Collectively, these social factors contribute to the delayed detection and removal of CSAM, thereby prolonging its circulation and compounding harm to children.

Owing to these gaps and challenges, victims bear the greatest burden, while Indian legislation continues to pay limited attention to victim rehabilitation. Taken together, these legal, technological and social limitations reflect deficiencies in the regulation and enforcement of provisions.

RECOMMENDATIONS

Adoption of Victim-Centric Terminology: Legislative reform should prioritise the use of the term child sexual abuse material (CSAM) in place of child pornography. This would reflect the

[26] Naveen Kumar, 'Circulation of child sexual abuse material rampant on Telegram' *THE HINDU* (Hyderabad, 16 November 2023) https://www.thehindu.com/news/national/telangana/circulation-of-child-sexual-abuse-material-rampant-on-telegram/article67536516.ece accessed 11 January 2026.

abusive nature of such content and align with international standards. This will help to strengthen victim-centric recognition.

Recognition of Transmission as a Continuous Offence: The legal framework should recognise transmission and circulation as a continuous threat rather than a one-time offence. It will help to reflect the realities of digital dissemination and the repeated victimisation of children.

Strengthening Intermediary Accountability: Intermediaries should be required to strictly comply with government advisories, statutory obligations and due diligence requirements. Effective enforcement mechanisms are necessary to ensure timely reporting and removal of CSAM. It will help to prevent platforms from evading responsibility under safe harbour protection.

Effective Implementation and Judicial Engagement: Beyond statutory provisions, effective implementation of existing laws is essential. Judicial precedents can play a significant role in interpreting legislative intent, addressing enforcement gaps and strengthening accountability in cases involving CSAM circulation.

Institutional Co-ordination and Policy Development: There is a need to strengthen institutional mechanisms through specialised committees and policy frameworks. Such efforts should be guided by expert recommendations focusing on prevention, victim rehabilitation and technological challenges. These coordinated efforts can contribute to a more comprehensive and responsive child protection strategy.

CONCLUSION

CSAM circulation poses a serious threat to children as it constitutes a form of continuous harm. Its permanent nature leads to revictimisation of the child with every instance of access, viewing or sharing. Unlike conventional forms of abuse, the circulation of CSAM extends the impact of the offence far beyond the initial act.

Although India has enacted various legal provisions to address CSAM, particularly under the Information Technology Act and the POCSO Act, these laws primarily focus on criminalising acts such as storage, possession and distribution. The existing framework remains largely

punitive in nature, concentrating on punishment after the commission of the offence rather than on preventing further harm through effective control of circulation.

Several gaps and challenges continue to facilitate the spread of CSAM. The rapid evolution of technology, coupled with features such as anonymity and end-to-end encryption, makes detection and removal increasingly difficult. In addition, inadequate due diligence by intermediaries, delays in reporting and content removal and lack of effective monitoring mechanisms further aggravate the problem. The absence of a victim-centric approach also contributes to underreporting, delaying timely intervention and allowing continued circulation.

These concerns highlight the need for updated and robust regulatory mechanisms to address CSAM effectively. Greater emphasis on awareness, digital literacy and preventive measures is essential to reduce vulnerability and reporting barriers. Most importantly, the implementation of existing provisions must be guided by the principle that child protection and the best interests of the child remain paramount in the digital space.