Page: 370-402 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 4

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.390

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)
To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript Click here

PROTECTION OF CHILDREN IN CYBERSPACE: A DOCTRINAL STUDY OF INDIAN LAW

Shruthi Sarang S Kamath*

I. ABSTRACT

The rapid expansion of digital technologies has transformed children's access to education, communication and entertainment. It has also exposed them to cyberbullying, online grooming, child sexual exploitative and abuse material (CSEAM), privacy violations, identity theft and AI-enabled threats. In India, the Information Technology Act, 2000[1], the Protection of Children from Sexual Offences Act, 2012[2], the Digital Personal Data Protection Act, 2023[3] and the new criminal laws address many of these harms, but their application to evolving forms of online harm remains uneven and, in part, untested. This study traces the evolution of Indian law on children's protection in cyberspace and evaluates how effectively it responds to existing and emerging cybercrimes, with particular attention to children's rights. It examines the principal legal and practical challenges, including definitional gaps, the accountability of intermediaries, the proof of electronic evidence and the deferred commencement of the child-specific data protection safeguards, which take effect only on 13 May 2027. The study adopts a doctrinal method. It relies on statutes, subordinate legislation and decisions of the Supreme Court as primary sources, and on books, journal articles and official reports as secondary sources. The study also draws on the UN Committee on the Rights of the Child's General Comment No. 25 (2021)[4] on children's rights in relation to the digital environment, which calls on States to adopt legislative and administrative measures to protect children's rights online and to legislate specifically where existing laws are inadequate. It concludes that the Indian framework covers most conduct that has moved from the

* 9th Semester Student of B.A. LL.B. (Hons.) at SASTRA Deemed University, India.
Email: sarangshruthi03@gmail.com

[1] Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
[2] Protection of Children from Sexual Offences Act, No. 32 of 2012, Acts of Parliament, 2012 (India).
[3] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
[4] Comm. 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 (Mar. 2, 2021).

© 2026. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

offline to the online world, but that specific gaps remain in definitions, intermediary accountability, implementation and enforcement.

II. KEYWORDS

Child Online Safety; POCSO Act, 2012; IT Act, 2000; DPDP Act, 2023; AI-Generated CSEAM.

III. INTRODUCTION AND RESEARCH PROBLEM

Children around the world have become among the most active users of the Internet and its services. Digital technologies play an important part in the lives of most children, and children's access to them is rising rapidly, with both beneficial and harmful effects[5]. The internet offers opportunities for learning, communication, entertainment and social interaction. However, the same openness exposes children to age-inappropriate material and to a range of online risks[6], including cyberbullying, online grooming, CSEAM, privacy violations, identity theft and AI-enabled threats.

In India, a set of separate statutes, rather than a single law, protects children in cyberspace. The Information Technology Act, 2000 (IT Act) addresses cyber offences. The Protection of Children from Sexual Offences Act, 2012 (POCSO Act) provides specific protection against sexual offences involving children. The Digital Personal Data Protection Act, 2023 (DPDP Act) regulates the processing of children's personal data. The Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) form the criminal justice framework, including the rules on the collection and proof of electronic evidence.

Although this framework exists, technological change has produced new forms of online harm that do not fit neatly within it. Artificial intelligence, deepfakes, synthetic content

[5] Sumedha Gupta, *Child's Right in Cyberspace: A Critical Analysis of Protection and Privacy under the Indian Legal System*, 4 Int'l J. Legal Sci. & Innovation 148 (2022).
[6] Sadhna Singh, *Online Safety for Children: Protecting the Next Generation from Harm*, NITI Aayog (June 2025), https://www.niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf.

and increasingly complex methods of online exploitation raise questions about the adequacy, clarity and adaptability of the existing law.

A. Literature Review

The literature relevant to this study falls into five themes.

1. **Children's rights in digital spaces:** Choudhuri[7] treats children not only as vulnerable users who require protection but also as holders of rights to participation, provision and protection in the digital environment. Verma, Kumar and Singhal[8] apply a similar lens to the IT Act, the POCSO Act and the DPDP Act and identify implementation difficulties, low digital literacy and weak enforcement. This literature supplies a rights-based foundation. However, Choudhuri's analysis predates the DPDP Act, and neither work examines how the statutes interact at the level of specific provisions.
2. **Cyberbullying and online delinquency:** Kumar and Ronghangpi[9] examine the forms, causes and effects of cyberbullying and note the absence of a comprehensive, child-specific legal response. Shivani Verma[10] adopts a psycho-legal approach to children's online behaviour under the BNS, the IT Act and the POCSO Act, and proposes combining legal regulation with awareness, parental involvement and technological safeguards. These works establish that cyberbullying falls between several statutes, but they do not map particular forms of conduct to particular provisions.

[7] Aratrika Choudhuri, *Conceptualising Children's Rights in Digital Spaces: Emerging Issues and Challenges*, 15 Socio-Legal Rev. 151 (2019), https://doi.org/10.55496/NTPF6562.
[8] Vijeta Verma et al., *Safeguarding Children's Rights in the Digital Age: A Critical Analysis of India's Cyber Laws*, *in* Child Protection Laws and Crime in the Digital Era ch. 11 (Romil Rawat ed., 2025), https://doi.org/10.4018/979-8-3373-5132-2.ch011.
[9] Naveen Kumar & Madhusmita Ronghangpi, *Cyber-bullying of Children: Impacts and Deterrent Measures in India*, 5 Indian J. Educ. Tech. 134 (2023), https://journals.ncert.gov.in/IJET/article/view/420.
[10] Shivani Verma, *A Psycho-Legal Analysis of Cyber Behaviours of Children: Legal Responses to Online Delinquencies*, 8 Indian J. Educ. Tech. 225 (2026), https://journals.ncert.gov.in/IJET/article/view/1778.

3. **Online sexual exploitation:** Manoj et al.[11] analyse India's response to online child sexual abuse and exploitation under the POCSO Act, the IT Act and the Juvenile Justice (Care and Protection of Children) Act, 2015, and compare it with international approaches. Their work confirms that sexual exploitation is among the gravest online harms to children, but it does not consider grooming, identity theft or data protection within the same frame.
4. **Privacy and data protection:** Gupta[12] analyses the protection and privacy of children in cyberspace under the Indian legal system. Because the work appeared in 2022, before the DPDP Act and the Digital Personal Data Protection Rules, 2025, it could not assess verifiable parental consent or the deferred commencement of these safeguards.
5. **AI-generated CSEAM:** Garg and Shukla[13] examine India's techno-legal response to AI-generated CSEAM and therefore engage directly with the threat that this study treats as emerging. Their analysis predates the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, which now regulate synthetically generated information.

The literature therefore shows that children face multiple forms of online harm and that several legal instruments address them. It remains fragmented by theme: studies concentrate on cyberbullying, on sexual exploitation or on children's digital rights and data protection, and few examine the relevant provisions of all the statutes together.

[11] Daniel Manoj et al., *Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation*, 4 Child Prot. & Prac. 100088 (2025).
[12] Sumedha Gupta, *Child's Right in Cyberspace: A Critical Analysis of Protection and Privacy under the Indian Legal System*, 4 Int'l J. Legal Sci. & Innovation 148 (2022).
[13] 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., no. 1, 2025, at 1, https://doi.org/10.55496/SZWH4909.

B. Research Gap

Existing studies have examined individual aspects of children's online safety, including cyberbullying, sexual exploitation, privacy and data protection, and recent scholarship has begun to address AI-generated CSEAM. What remains missing is a single doctrinal account of how the IT Act, the POCSO Act, the DPDP Act and the BNS, BNSS and BSA interact at the level of specific provisions after the Digital Personal Data Protection Rules, 2025 and the 2026 amendment to the intermediary rules. This study also assesses that framework from a children's rights perspective, in light of General Comment No. 25 (2021) of the UN Committee on the Rights of the Child on children's rights in relation to the digital environment.

C. Research Problem

The principal problem that this study addresses is whether the existing Indian legal framework adequately protects children from existing and emerging cybercrimes while safeguarding their rights and best interests in cyberspace.

The framework is fragmented, which makes it difficult to determine how the different laws apply and interact. Further challenges include the collection and proof of digital evidence, cross-border offending, low technological literacy and rapidly evolving forms of AI-enabled harm.

D. Significance of the Study

The study is significant because children are a nation's asset, and crimes against them committed through cyberspace are a serious concern[14]. National Crime Records Bureau (NCRB) data show that cybercrimes against children rose from 1,376 cases in 2021 to 1,823 cases in 2022, an increase of about 32 per cent[15]. The latest NCRB report, *Crime in India*

[14] S. Sarkar, The Silent Victims of Cyber Space: Analyzing Cyber-Crimes Against Children in the Indian Context (2026) (unpublished LL.M. dissertation, Kazi Nazrul University).
[15] DTE Staff, *Over 1,800 Cases of Cybercrimes Against Children Registered in 2022, Higher Than Last Year: NCRB*, Down To Earth (Dec. 6, 2023), https://www.downtoearth.org.in/governance/over-1-800-cases-of-cybercrimes-against-children-registered-in-2022-higher-than-last-year-ncrb-93236.

2024, records 1,87,702 crimes against children in 2024, a rise of 5.8 per cent over 2023, and 1,238 cases registered under the IT Act as cybercrimes against children, of which 1,099 involved publishing or transmitting material depicting children in sexually explicit acts[16]. Because the 2024 figure counts only cases registered under the IT Act, it is not directly comparable with the earlier totals; the data nonetheless confirm that sexually explicit material is the dominant form of cybercrime against children.

Children's growing dependence on digital technology therefore calls for legal protection that responds to both existing and emerging cyber offences. It is accordingly pertinent to examine the interaction between cybercrime law, child protection law and data protection law in order to identify the gaps in the existing legal system.

E. Aim, Scope and Limitations of the Study

The study aims to examine the effectiveness of the Indian legal framework in protecting children from established and emerging cybercrimes, and to identify the legal and practical gaps that require legislative or regulatory reform for the protection of children's rights and best interests in cyberspace.

The study focuses on Indian law, namely the IT Act and the intermediary rules made under it, the POCSO Act, the DPDP Act and the Digital Personal Data Protection Rules, 2025, and the relevant provisions of the BNS, BNSS and BSA. It also considers decisions of the Supreme Court and General Comment No. 25. Because technology develops rapidly, certain threats and regulatory responses may continue to evolve during and after the study. The law is stated as at November 2026.

F. Research Objectives

The objectives of this study are:

[16] National Crime Records Bureau, Ministry of Home Affairs, *Crime in India 2024* (2026); *see also 1,87,702 Cases of Crimes Against Children Recorded in 2024: NCRB Data*, Deccan Herald (2026), https://www.deccanherald.com/india/187702-cases-of-crimes-against-children-recorded-in-2024-ncrb-data-3995822.

1. To trace the evolution of Indian law relating to children's protection in cyberspace;
2. To analyse the relevant provisions of the IT Act, the intermediary rules and the POCSO Act;
3. To examine the relevance of the DPDP Act, the Digital Personal Data Protection Rules, 2025 and the new criminal laws;
4. To identify existing and emerging cybercrimes that affect children;
5. To analyse the challenges relating to intermediary accountability, digital evidence and enforcement against offenders and platforms located outside India; and
6. To identify the legal and regulatory measures required to strengthen child protection in cyberspace.

G. Research Questions

The principal research question is whether the existing Indian legal framework adequately protects children from existing and emerging cybercrimes while safeguarding their rights and best interests in cyberspace. The subsidiary questions are:

1. Which provisions of the IT Act, the POCSO Act and the BNS apply to cyberbullying, grooming, CSEAM, identity theft and privacy violations against children?
2. How far do the intermediary rules and the DPDP Act protect children's safety and personal data online?
3. Do the existing definitions extend to AI-generated and synthetic material?

H. Research Methodology

The study adopts a doctrinal research methodology. The primary sources are statutes, subordinate legislation, decisions of the Supreme Court and General Comment No. 25 (2021). The secondary sources are books, journal articles, research papers and official reports. The study analyses the relevant provisions through statutory interpretation and

judicial analysis, and identifies gaps by applying those provisions to existing and emerging cybercrimes affecting children.

IV. RESEARCH AND ANALYSIS

A. Indian Legal Framework and its Evolution

The growing use of the internet by children has created both opportunities and risks. Digital platforms give children access to education, information, entertainment and communication, but they also expose them to cyberbullying, online grooming, sexual exploitation, CSEAM, identity theft, privacy violations and AI-enabled threats. The legal protection of children in cyberspace is spread across several statutes and regulatory instruments[17].

The framework developed in stages. Parliament enacted the IT Act in 2000 primarily to give legal recognition to electronic commerce; the Act acquired most of its cybercrime provisions through the Information Technology (Amendment) Act, 2008, which inserted Sections 66C, 66D, 66E, 67A and 67B[18]. Parliament enacted the POCSO Act in 2012 and amended it in 2019 to define child pornography in Section 2(1)(da) and to restructure the offences in Sections 14 and 15[19].

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 imposed due-diligence duties on platforms[20], and a 2026 amendment extended those duties to synthetically generated information[21]. In 2023, Parliament enacted the DPDP Act and replaced the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973 and the Indian Evidence Act, 1872 with the BNS, BNSS and BSA, which

[17] Ankit Sourav Sahoo, *The Legal Lacunae in Protecting Children from Cyber-Bullying and Grooming in India*, 4 J. Advance & Future Res. 120 (2026), https://rjwave.org/jaafr/papers/JAAFR2603615.pdf.
[18] Information Technology (Amendment) Act, No. 10 of 2009 (India).
[19] Protection of Children from Sexual Offences (Amendment) Act, No. 25 of 2019 (India).
[20] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India).
[21] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).

came into force on 1 July 2024. The Digital Personal Data Protection Rules, 2025 began a phased commencement of the DPDP Act that will be complete only on 13 May 2027[22].

The principal statutes that protect children in cyberspace are therefore the IT Act, the POCSO Act, the DPDP Act and the new criminal laws. The IT Act provides for several technology-related offences and their remedies[23]. The POCSO Act focuses on protecting children from all forms of sexual offences[24]. This part examines how these laws apply to the cybercrimes that affect children and identifies the gaps in the existing framework[25].

B. Cybercrimes that Affect Children

The major cybercrimes that affect children are the following.

1. **Cyberbullying:** Cyberbullying refers to bullying through digital technologies[26]. It comprises repeated harassment, threats, humiliation or intimidation. Children may receive abusive messages, suffer public humiliation, have private information circulated, be impersonated or be excluded from online groups. Indian law contains no offence of cyberbullying as such. Since the Supreme Court struck down Section 66A of the IT Act in *Shreya Singhal v. Union of India*[27], no general offence of sending offensive online messages exists, and cyberbullying must be mapped to specific provisions. These include Sections 75 (sexual harassment), 78 (stalking), 351 (criminal intimidation) and 356 (defamation) of the BNS, which correspond to Sections

[22] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1 (Nov. 13, 2025) (India).
[23] K. Jaishankar & T. Divya, *Cyber Offences under the Information Technology Act*, e-PG Pathshala, https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S001608/P001742/M022125/ET/1504245749E-Text-ITAct-JaishankarDivya.pdf.
[24] *Protection of Children from Sexual Offences Act, 2012*, Tamil Nadu State Judicial Academy, https://www.tnsja.tn.gov.in/article/pocso_material.pdf.
[25] Lina Acca Mathew, Legislative Models of Prosecuting Child Sexual Abuse in India: A Review and Critical Analysis (July 2017) (Ph.D. dissertation, Queensland University of Technology) (on file with QUT ePrints), https://doi.org/10.5204/thesis.eprints.107784.
[26] *Cyberbullying: What Is It and How to Stop It*, UNICEF (Jan. 2026), https://www.unicef.org/stories/how-to-stop-cyberbullying.
[27] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

354A, 354D, 503 and 506, and 499 and 500 of the Indian Penal Code, 1860[28]. Sections 75 and 78 of the BNS, however, identify the victim as a woman. Because Section 2(35) of the BNS defines a woman as a female human being of any age, these provisions protect girls but not boys, a gap of direct relevance to child protection. Where the bullying is sexual in nature, Section 11 of the POCSO Act, which is gender-neutral, fills part of this gap. Sections 66C (identity theft) and 67 (obscene material) of the IT Act apply only where the bullying involves the misuse of credentials or obscene content. Depending on the facts, cyberbullying may therefore fall under several provisions of different statutes, which makes a uniform legal response difficult[29].

2. **Online Grooming:** Online child grooming is the act of developing a relationship with a child to enable the child's abuse and exploitation both online and offline[30]. It typically involves sexual communication with a minor[31]. An offender may first build trust through social media, gaming platforms or messaging applications and then gradually seek personal information, photographs or sexual content. Grooming is difficult to address because the harmful conduct develops over time and may not initially appear criminal. Indian law nonetheless contains relevant offences. Section 67B(c) of the IT Act punishes anyone who "cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act" or in a manner that may offend a reasonable adult[32]. This is the closest existing offence to grooming, although its reference to a relationship "with one or more

[28] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 75, 78, 351, 356 (India).
[29] Divya Yadav, *Cyberbullying Laws in India: Current Challenges and Reforms*, 2 Int'l J. Legal Res. & Analysis, no. 7, Mar. 2025, at 23, https://www.ijlra.com/details/cyberbullying-laws-in-india-current-challenges-and-reforms-by-divya-yadav.
[30] *What Is Online Child Sexual Abuse and Exploitation?*, CEOP Safety Centre, https://ceop.police.uk (last visited Sept. 30, 2026).
[31] S. Wefers et al., *Understanding and Deterring Online Child Grooming: A Qualitative Study*, 19 Sex Offending, art. e13147 (2024).
[32] Information Technology Act, No. 21 of 2000, § 67B(c) (India); Protection of Children from Sexual Offences Act, No. 32 of 2012, § 11 (India).

children" fits awkwardly where the adult offender is the other party. Section 11 of the POCSO Act treats as sexual harassment the act of repeatedly contacting a child through electronic or digital means, and of enticing a child for pornographic purposes, when done with sexual intent. The gap lies elsewhere: no statute defines "grooming", and the existing offences reach preparatory conduct only when it already has a sexual or pornographic object. Early trust-building aimed at later abuse falls outside them.

3. **Child Sexual Exploitative and Abuse Material (CSEAM):** CSEAM is among the most serious forms of online exploitation of children. It is the record of the sexual abuse or exploitation of a child. Technology has made the creation, storage, transmission and circulation of such material easier and allows it to reach a large audience[33]. Section 67B of the IT Act penalises a range of conduct relating to material depicting children in sexually explicit acts and other forms of online child sexual exploitation[34]. Sections 13, 14 and 15 of the POCSO Act address the use of children for pornographic purposes and the storage of such material[35]. Following the Supreme Court's direction, this paper uses the term CSEAM, except where it refers to the statutory expression "child pornography". In *Just Rights for Children Alliance v. S. Harish*[36], the Madras High Court had held that merely downloading and watching such material in private was not an offence[37]. On 23 September 2024, the Supreme Court set that decision aside. It held that "possession" under Section 15 of the POCSO Act

[33] *Module 12: Interpersonal Cybercrime: Online Child Sexual Exploitation and Abuse*, United Nations Office on Drugs and Crime, https://sherloc.unodc.org/cld/pt/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html (last visited Oct. 3, 2026).
[34] Information Technology Act, No. 21 of 2000, § 67B (India); *Cyber Safety Guideline*, National Commission for Protection of Child Rights, https://ncpcr.gov.in/public/index.php/viewPdf/16613369326305fd6444e1b_cyber-safety-guidline.pdf (last visited Oct. 25, 2026).
[35] S. Shukla et al., *Legal Complexities of Adolescent Relationships: A Study of Protection of Child Sexual Offense Cases in India*, 16 Cureus e60475 (2024).
[36] *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716 (India).
[37] *Id.* (setting aside the judgment of the High Court of Madras dated Jan. 11, 2024).

includes constructive possession: a person who views such material online without downloading it possesses it if he knowingly exercises control over it. Unknowing or accidental access does not by itself amount to possession, but a person who comes upon such material and fails to delete, destroy or report it may be liable under Section 15(1). The Court also directed all courts not to use the term "child pornography", endorsed the term "child sexual exploitative and abuse material", and suggested that Parliament amend the POCSO Act accordingly. As at November 2026, Parliament had not enacted that amendment.

4. **Identity Theft and Impersonation:** Identity theft is the fraudulent or dishonest use of the electronic signature, password or other unique identification feature of another person[38]. Children are increasingly its victims, as their identities can be used to create false social media accounts or to commit fraud[39]. Identity theft is a less visible but damaging cybercrime, because it can affect a child's future digital and financial identity[40]. Sections 66C and 66D of the IT Act punish identity theft and cheating by personation respectively, and Section 319 of the BNS punishes cheating by personation[41]. Where a child is the victim, investigating agencies can invoke these provisions together with any other applicable offence.
5. **Privacy Violation:** Children's privacy is engaged whenever information about them, such as their identity, activities, location, communications, emotions,

[38] *Learn About Cybercrime*, National Cybercrime Reporting Portal, Ministry of Home Affairs, Government of India, https://cybercrime.gov.in/webform/crimecatdes.aspx (last visited Sept. 30, 2026).
[39] Anurag Yadav & Kaur, *Confronting the Growing Threat of Child Identity Theft in the Age of Digitalisation* (2024).
[40] Milford D'Souza, *Understanding Cyber Crime Against Children: What You Need to Know*, CRY (Dec. 29, 2025), https://www.cry.org/blog/cyber-crime-against-children/.
[41] *Cyber Crime Offences in the Domain of Bharatiya Nyaya Sanhita (BNS) – 2023*, Indian Railways, https://ncr.indianrailways.gov.in/uploads/files/1749022724173-CYBER%20OFFENCES%20(BNS).pdf (last visited Oct. 25, 2026).

health or relationships, is collected, processed or disclosed[42]. Children often share photographs, location information, contact details and other personal information online without fully understanding the consequences[43]. Their privacy can also be violated through the recording or circulation of private images and the misuse of personal data[44]. Privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution[45]. A nine-judge bench of the Supreme Court recognised it as a fundamental right on 24 August 2017 in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[46]. The UN Committee on the Rights of the Child, in General Comment No. 25, states that privacy is vital to children's agency, dignity and safety and to the exercise of their rights, and calls on States to ensure that children's privacy and personal data are protected in the digital environment[47]. Section 23 of the POCSO Act protects the identity of a child victim from disclosure by the media[48]. Section 9 of the DPDP Act regulates the processing of children's personal data, although it takes effect only on 13 May 2027. Privacy protection is therefore not limited to preventing criminal activity; it also requires regulation of the collection and processing of children's data in the digital environment.

C. Specific Laws Dealing with Cybercrimes

1. Information Technology Act, 2000

[42] Comm. on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, ¶ 68, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).
[43] Efua Andoh, *What You Need to Know Before Sharing Your Child's Life Online*, Monitor on Psychology, June 1, 2026, at 24, https://www.apa.org/monitor/2026/06/parents-children-sharing-online.
[44] Nazuk Sood, *Data Protection Vis-À-Vis Right to Privacy*, 12 Int'l J. Res. & Sci. Innovation 1925 (2025).
[45] Shruthi Sarang S. Kamath, *Right to Privacy: Pre- and Post- Puttaswamy Developments*, *in* Emerging Trends in Constitutional Law and Human Rights Jurisprudence (Notion Press 2026).
[46] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[47] Comm. on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, ¶¶ 67, 70, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).
[48] Protection of Children from Sexual Offences Act, No. 32 of 2012, § 23 (India).

The IT Act is one of the principal statutes on technology-related offences. Sections 43 and 66 are relevant because they deal with contraventions and offences respectively.

- Section 43 imposes civil liability for acts such as unauthorised access, downloading, introducing viruses, disrupting computer systems and other damage to computer resources.
- Section 66 makes the acts in Section 43 an offence when they are committed dishonestly or fraudulently. Not every contravention of Section 43 is therefore an offence under Section 66, which requires a culpable mental state. These provisions apply when a child's computer or account is unlawfully accessed or manipulated.
- Section 66C punishes identity theft, that is, the fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature[49]. It applies where a child's credentials are stolen and misused.
- Section 66D penalises cheating by personation[50]. It applies when a person, by means of a communication device or computer resource, cheats by pretending to be another person, real or fictitious[51]. It therefore reaches an offender who creates a false identity to deceive a child. The provision does not address grooming as such: it reaches only deception that amounts to cheating, while Section 67B(c) addresses the sexual inducement itself.
- Section 66E punishes the intentional or knowing capture, publication or transmission of images of a person's private area without consent, in circumstances violating that person's privacy. It protects a child whose private images are captured, stored or circulated. Children's privacy,

[49] Rahul Kailas Bharati, Identity Theft and Impersonation in Cyberspace (Sections 66C and 66D of the IT Act, 2000) (July 24, 2025) (working paper), https://ssrn.com/abstract=5379783.
[50] Ch. Rajender Reddy & Srinivas M, *Cybercrime Against Women in India: Closing the Consent, Evidence and Enforcement Gaps*, 9 Int'l J.L. Mgmt. & Humanities 301 (2026), https://doi.org/10.63108/IJLMH.12835.
[51] Rahul Kailas Bharati, Identity Theft and Impersonation in Cyberspace (Sections 66C and 66D of the IT Act, 2000) (July 24, 2025) (working paper), https://ssrn.com/abstract=5379783.

however, extends beyond such images to the collection and tracking of personal data, which falls within data protection law.

- Section 67 penalises publishing or transmitting obscene material in electronic form. Children's heavy use of digital platforms makes exposure to such material a real risk to their psychological well-being.
- Section 67A penalises publishing or transmitting material containing sexually explicit acts in electronic form. A child who encounters such material on the many platforms he or she uses may suffer serious harm.
- Section 67B is the provision most directly concerned with children. It punishes anyone who (a) publishes or transmits material depicting children engaged in sexually explicit acts; (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material depicting children in an obscene, indecent or sexually explicit manner; (c) cultivates, entices or induces children to an online relationship for sexually explicit acts; (d) facilitates abusing children online; or (e) records in electronic form one's own abuse or that of others pertaining to sexually explicit acts with children. The punishment is imprisonment of up to five years and a fine of up to ten lakh rupees on first conviction, and imprisonment of up to seven years and a fine of up to ten lakh rupees on a subsequent conviction. A proviso excludes material proved to be justified as being for the public good, such as material in the interest of science, literature, art or learning, and material kept or used for bona fide heritage or religious purposes. Because clause (b) covers the creation of "digital images", it already reaches some computer-generated material.

The IT Act thus lays the foundation for addressing cyber offences that affect children. It was, however, enacted for an earlier technological environment, and it does not expressly

name AI-generated sexual content, deepfakes or AI-assisted grooming[52]. Section 67B(b) and the intermediary rules now carry much of this burden, as the next sub-section shows.

The proposed Digital India Act, intended to replace the IT Act, has not progressed beyond consultation, and the IT Act remains in force[53]. Its effectiveness therefore depends on proper enforcement, technological capacity, coordination with child protection and data protection law, and continued adaptation to emerging forms of cybercrime.

2. Intermediary Liability and Platform Obligations

Platforms are the most practical point of control over CSEAM and grooming. Section 79 of the IT Act grants intermediaries a safe harbour from liability for third-party content, provided that they do not initiate the transmission, select its receiver or modify its content, and that they observe due diligence[54]. In *Shreya Singhal*, the Supreme Court read down Section 79(3)(b), so that an intermediary must remove content only on actual knowledge of a court order or a notification by the appropriate government[55]. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 build on this position. Rule 3(1)(b) requires intermediaries to make reasonable efforts to prevent users from hosting obscene, paedophilic or child-harmful content, and Rule 4(4) requires significant social media intermediaries to endeavour to deploy automated tools to identify material depicting child sexual abuse[56].

The 2026 amendment, notified on 10 February 2026 and in force from 20 February 2026, extends these duties to "synthetically generated information". It reduces the time for removing unlawful content after a court order or government direction from 36 hours to

[52] 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., no. 1, 2025, at 1, https://doi.org/10.55496/SZWH4909.
[53] *Govt Held First Public Consultation on Proposed Digital India Act*, ThePrint (Mar. 10, 2023), https://theprint.in/economy/govt-held-first-public-consultation-on-proposed-digital-india-act/1432385.
[54] Information Technology Act, No. 21 of 2000, § 79 (India).
[55] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
[56] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), rr. 3(1)(b), 4(4) (Feb. 25, 2021) (India).

three hours, and requires the removal of non-consensual intimate imagery, including morphed or deepfake images, within two hours of a complaint. Intermediaries that offer tools for creating synthetic content must deploy technical measures to prevent the generation of synthetic CSEAM and must label lawful synthetic content[57].

Enforcement against foreign platforms remains the weak point. Most large platforms are incorporated abroad and store data outside India, so investigators often depend on voluntary disclosure by the platform or on a letter of request issued by a court under Section 112 of the BNSS, which is a formal and often lengthy process[58]. In the absence of new legislation, the intermediary framework currently carries the principal regulatory response to online harm against children.

3. Protection of Children from Sexual Offences Act, 2012

The POCSO Act was enacted to protect persons below eighteen years of age from sexual offences and to establish Special Courts[59] to try such offences[60]. It is central to cybercrime against children because several forms of sexual exploitation now take place through digital environments.

Section 11 defines sexual harassment of a child. When done with sexual intent, it includes showing a child any object in any form or media for pornographic purposes; repeatedly or constantly following, watching or contacting a child directly or through electronic, digital or any other means; threatening to use a real or fabricated depiction of the child through electronic, film or digital media; and enticing a child for pornographic purposes.

---

[57] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India) (amending rr. 2, 3 and 4).
[58] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 112 (India).
[59] Ranjana Ferrao, *Special Courts for Children: Lessons Learnt from India*, 15 Int'l J. Ct. Admin., no. 2, 2024, art. 7, https://iacajournal.org/articles/10.36745/ijca.485.
[60] P. Rahul Ambedkar, *Protection of Children from Sexual Offences Act, 2012 – An Overview*, Kerala Judicial Academy (Sept. 2024), https://cdnbbsr.s3waas.gov.in/s3ec030b6ace9e8971cf36f1782aa982a7/uploads/2024/09/2024092050.pdf .

The express reference to electronic and digital means makes Section 11 relevant to online sexual harassment and to certain forms of online grooming.

Section 2(1) (da), inserted in 2019, defines child pornography as "any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer-generated image indistinguishable from an actual child, and image created, adapted, or modified, but appear to depict a child". This is the key provision on synthetic content. Its second and third limbs reach morphed and computer-generated images, so the law does not leave AI-generated material wholly unregulated. Three interpretive questions remain. First, the Act does not define "indistinguishable from an actual child", and it is unclear whether stylised or cartoon-like images fall within it. Second, the definition speaks of conduct "involving a child", which leaves room to argue that fully synthetic images depicting no real child fall outside it. Third, courts have yet to decide how far the offences in Sections 13 to 15 reach such material. Section 67B(b) of the IT Act, which covers anyone who "creates text or digital images", supplies a parallel basis for liability. The problem is therefore one of interpretation and enforcement, not a definitional vacuum.

Section 13 defines the offence of using a child for pornographic purposes. It covers the use of a child in any form of media, including programmes or advertisements on television, the internet or any other electronic form, for sexual gratification, including the representation of a child's sexual organs, the use of a child in real or simulated sexual acts and the indecent or obscene representation of a child.

Section 14 prescribes the punishment for that offence: imprisonment of not less than five years and a fine, and not less than seven years and a fine on a subsequent conviction, with additional punishment where the offender also commits a sexual assault on the child[61]. It complements Section 67B of the IT Act.

[61] Protection of Children from Sexual Offences Act, No. 32 of 2012, § 14 (India) (as substituted by Act No. 25 of 2019).

Section 15 creates three distinct offences of storage or possession. Sub-section (1) punishes storing or possessing such material with an intention to share or transmit it, shown by failing to delete, destroy or report it to the designated authority; the punishment is a fine of not less than five thousand rupees, and not less than ten thousand rupees for a subsequent offence. Sub-section (2) punishes storing or possessing such material for transmitting, propagating, displaying or distributing it, except for reporting or for use as evidence in court, with imprisonment of up to three years, a fine, or both. Sub-section (3) punishes storing or possessing such material for commercial purposes with imprisonment of three to five years, a fine, or both, on first conviction, and five to seven years with a fine on a subsequent conviction[62]. Each limb therefore turns on a different mental element: an intention to share inferred from inaction, an intention to transmit, and a commercial purpose.

In *Harish*[63], the Supreme Court read Section 15 together with Section 67B of the IT Act. It treated the offences in Section 15 as inchoate offences that punish possession with the requisite intention, held that this intention may be inferred from the manner of storage or from the failure to delete or report, and applied the statutory presumption of a culpable mental state under Section 30. The decision shows how judicial interpretation can adapt existing provisions to material stored on devices or in the cloud, or accessed without download.

4. Digital Personal Data Protection Act, 2023

The DPDP Act introduces a specific statutory framework for processing digital personal data and adds an important privacy dimension to the protection of children online.

Section 9 governs the processing of children's personal data. Section 2(f) defines a child as an individual who has not completed eighteen years of age, and Section 2(j) includes the child's parents or lawful guardian within the term "data principal". Before processing

[62] Protection of Children from Sexual Offences Act, No. 32 of 2012, § 15 (India) (as substituted by Act No. 25 of 2019).
[63] *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716 (India).

a child's personal data, a data fiduciary must obtain the verifiable consent of the parent of the child or the lawful guardian, as the case may be[64]. It must not process personal data in a manner likely to cause any detrimental effect on the well-being of a child, and must not undertake tracking, behavioural monitoring or targeted advertising directed at children. Under Section 9(4) and (5), the Central Government may exempt classes of data fiduciaries or purposes from these obligations, and may notify an age above which a data fiduciary whose processing is verifiably safe is exempt.

Section 9 is not yet operative. The Digital Personal Data Protection Rules, 2025, notified on 13 November 2025, bring the Act into force in phases, and Section 9 and the child-specific Rules take effect only on 13 May 2027[65]. Rule 10 requires a data fiduciary to verify that the person giving consent is an identifiable adult, by reference to reliable identity and age details already available to it, or details or a virtual token voluntarily provided through an authorised entity such as a digital locker. Rule 11 sets out a parallel mechanism for persons with disabilities who have a lawful guardian. Rule 12, read with the Fourth Schedule, exempts specified classes of data fiduciaries, such as clinical establishments, educational institutions and child-care centres, and specified purposes from the consent requirement and the restriction on tracking. A Removal of Difficulties Order made in October 2026 corrected the wording of Section 9(1) without altering its commencement[66].

[64] Digital Personal Data Protection Act, No. 22 of 2023, §§ 2(f), 2(j), 9 (India); Shreya Suri & Vikram Jeet Singh, *Processing of Children's Personal Data under the DPDP Act: What Does It Mean for Businesses?*, ELP Law (Aug. 23, 2024), https://elplaw.in/leadership/processing-of-childrens-personal-data-under-the-dpdp-act-what-does-it-means-for-businesses-3/.

[65] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), rr. 1, 10, 11, 12 & sch. 4 (Nov. 13, 2025) (India).

[66] Digital Personal Data Protection (Removal of Difficulties) Order, 2026, S.O. 5458(E) (Oct. 5, 2026) (India).

The need for child-specific data protection arises from the growing volume of information that digital platforms collect from children[67], including identity and contact details, behavioural information, preferences and other digital activity.

The DPDP Act is therefore relevant to profiling, targeted advertising and tracking, risks that traditional cybercrime law does not reach. Its child-specific safeguards nonetheless raise practical problems. Verifying age and parentage at scale may require platforms to collect more identity data from both children and parents. A uniform parental-consent requirement for every person below eighteen also sits uneasily with an adolescent's own privacy and right of access to information, which General Comment No. 25 emphasises. Until May 2027, these safeguards remain prospective.

5. New Criminal Laws

The BNS, BNSS and BSA came into force on 1 July 2024 and form the current criminal justice framework. The BNS supplies the substantive offences that apply to online harm against children, notably Sections 75, 78, 351 and 356, discussed above, and Section 319 on cheating by personation.

Evidence is paramount in cybercrimes involving children, because digital communications, social media records, electronic files and device data usually constitute the proof of the offence. The BNSS strengthens its collection. Section 94 empowers a court or police officer to require the production of any document or electronic communication, including a communication device likely to contain digital evidence; Section 105 requires search and seizure to be recorded through audio-video electronic means; and Section 176(3) requires a forensic expert to visit the crime scene for offences punishable with seven years' imprisonment or more[68]. Where evidence is held abroad, a court may issue a letter of request under Section 112.

[67] Navonita Mallick et al., *Children's Data Protection in Smart Educational Platforms: Addressing Privacy Risks in Intelligent Communication Systems*, 2025 AI Summit 294, 296 (2025).
[68] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 94, 105, 112, 176(3) (India).

© 2026. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

Section 63 of the BSA replaces Section 65B of the Indian Evidence Act, 1872[69]. A secondary electronic record is admissible only with a certificate in the form prescribed in the Schedule: Part A is completed by the party or the person in charge of the device and Part B by an expert, and the certificate must disclose the hash value of the record. The rule builds on *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, in which the Supreme Court held that the certificate is a mandatory condition for admitting secondary electronic evidence[70].

In May 2026, the Supreme Court upheld the validity of Section 63(4) and the Schedule, and declined to treat as binding a High Court view that only examiners notified under Section 79A of the IT Act may sign Part B[71]. For child victims, these requirements govern evidence from seized devices, cloud accounts and foreign platforms, and procedural lapses can defeat otherwise strong cases. Laws against cybercrime work only when investigators can lawfully collect, preserve and prove digital evidence.

6. Children's Rights in the Digital Environment

Protection from cybercrime is only one part of children's rights in cyberspace. Children also have rights to privacy, education, access to information, expression and participation, and to protection from exploitation.

General Comment No. 25 calls on States to take legislative, administrative and other measures to protect children's rights in the digital environment[72]. To give effect to it, India must ask not only whether its cyber laws protect children, but also whether they enable children to exercise their rights safely in the digital environment.

---

[69] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63 & sch. (India).
[70] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India); *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
[71] *Pune Bar Ass'n v. Union of India*, W.P. (C) No. 599 of 2026, 2026 LiveLaw (SC) 551 (India) (order dated May 22, 2026).
[72] Rita Ozoemena, *General Comment No. 25 on Children's Rights in Relation to the Digital Environment: Implications for Children's Right to Privacy and Data Protection in Africa*, 24 Hum. Rts. L. Rev. ngae018 (2024).

D. Emerging AI-Enabled Cyber Threats

Artificial intelligence has created new obstacles to protecting children in cyberspace. AI tools can create or manipulate images, audio and video and can facilitate intricate forms of online deception. A principal concern is the creation of synthetic sexualised images of children: deepfake technology allows any person to alter an existing image or video, or to generate a new one, that appears real. Other risks include AI-assisted grooming, voice cloning used for impersonation or sextortion, and automated manipulation.

Indian law already addresses these threats in part. Section 2(1)(da) of the POCSO Act and Section 67B(b) of the IT Act reach computer-generated and digitally created images of children. Since 20 February 2026, the amended intermediary rules have defined "synthetically generated information" as audio, visual or audio-visual information artificially or algorithmically created or altered so that it appears real. They require platforms that offer AI tools to prevent the generation of synthetic CSEAM, to label lawful synthetic content with visible markers and embedded provenance metadata, and to remove unlawful content within three hours of a lawful order[73]. Voice cloning and AI-assisted sextortion fall under Sections 66C and 66D of the IT Act and Sections 308 (extortion) and 319 of the BNS, and AI-assisted grooming falls under Section 67B(c) of the IT Act and Section 11 of the POCSO Act.

Three real gaps remain. First, where an image depicts no real child, a prosecution must rely on the "indistinguishable" and "appear to depict" limbs of Section 2(1)(da), which courts have not yet interpreted. Second, attributing AI-generated material to a particular person is technically difficult, particularly where open-source models run on private devices. Third, the intermediary rules bind platforms that serve Indian users, but Indian law contains no offence specifically directed at those who develop or distribute models built to generate CSEAM. The United Kingdom illustrates a direct response: its Crime and Policing Act 2026 creates an offence of making, adapting, possessing or supplying a

[73] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), r. 2(1)(wa) (Feb. 10, 2026) (India).

"child sexual abuse image-generator"[74]. Indian scholarship has begun to examine these questions[75].

E. Analysis of the Existing Legal Framework

The Indian legal framework has several strengths. The IT Act addresses identity theft, cheating by personation and privacy violations[76], as well as material depicting children in sexually explicit acts, including online inducement under Section 67B(c)[77]. The POCSO Act is child-specific and gender-neutral, expressly covers sexual harassment through electronic means, and its 2019 definition in Section 2(1)(da) extends to computer-generated images. The intermediary rules, as amended in 2026, impose concrete prevention and takedown duties on platforms. The DPDP Act will add child-specific data safeguards from May 2027. Finally, *Harish* shows that courts can interpret existing provisions in response to digital forms of misuse.

At the same time, the framework remains fragmented, and many forms of online harm require the application of several statutes. Five concerns stand out. First, no statute defines grooming or cyberbullying, and Sections 75 and 78 of the BNS protect only female victims. Second, the application of Section 2(1) (da) to wholly synthetic images remain untested. Third, effective enforcement requires trained investigators, cyber-forensic experts and compliance with the certificate requirement under Section 63 of the BSA. Fourth, cross-border offending and foreign platforms complicate investigation. Fifth, protective measures should not result in surveillance of children's personal information;

[74] Crime and Policing Act 2026, c. 20, § 72 (UK) (inserting § 46A into the Sexual Offences Act 2003; not in force on Royal Assent).
[75] 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., no. 1, 2025, at 1, https://doi.org/10.55496/SZWH4909.
[76] Information Technology Act, No. 21 of 2000, §§ 66C, 66D, 66E, 67B (India).
[77] Gaurav Saluja, *Critical Assessment of Information Technology Act, 2000*, Legal Service India (Apr. 29, 2023), https://www.researchgate.net/publication/370375309_Critical_Assessment_of_Information_Technology_Act_2000.

they must be balanced with children's rights to privacy, participation and access to information.

F. Findings and Discussion

The study finds that the Indian framework is largely adequate for conduct that has moved from the offline to the online world, but not yet adequate for the protection of children in cyberspace as a whole. The IT Act and the POCSO Act cover most forms of cyber-enabled sexual exploitation, including grooming with a sexual object and, in principle, computer-generated material. The gaps are specific and identifiable: a definitional gap, because no statute defines grooming or cyberbullying and Sections 75 and 78 of the BNS are gender-specific; interpretive uncertainty over wholly synthetic CSEAM under Section 2(1)(da) of the POCSO Act; limited intermediary accountability, particularly against foreign platforms and AI-model providers; an implementation gap, because Section 9 of the DPDP Act and Rule 10 take effect only on 13 May 2027[78]; and an enforcement gap in forensic capacity and the proof of electronic evidence. Effective protection of children in cyberspace therefore requires a combination of legal, technological and rights-based measures.

V. SUGGESTIONS AND RECOMMENDATIONS

The study shows that India has a substantial framework for protecting children in cyberspace, but rapid technological change has exposed specific gaps. The following recommendations address them.

1. **Define online grooming:** Parliament should insert an express definition of online grooming in Section 67B of the IT Act or in the POCSO Act, covering communication with a child intended to facilitate sexual abuse even before any sexual content is sought. It should also make Sections 75 and 78 of the BNS gender-neutral where the victim is a child.

[78] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), rr. 1, 10 (Nov. 13, 2025) (India).

2. **Adopt CSEAM terminology and clarify synthetic material:** As the Supreme Court suggested in *Harish*, the Ministry of Women and Child Development should bring forward an amendment replacing "child pornography" with "child sexual exploitative and abuse material" in the POCSO Act, and should clarify that Section 2(1) (da) covers wholly synthetic images that depict no real child.
3. **Strengthen intermediary duties:** The Ministry of Electronics and Information Technology should amend the intermediary rules to prescribe a time limit within which platforms must report detected CSEAM and grooming to the National Cybercrime Reporting Portal, and to require platforms to publish child-safety transparency data.
4. **Sequence data protection compliance with children's access:** Before Rule 10 takes effect, the Ministry of Electronics and Information Technology and the Data Protection Board of India should issue guidance on privacy-preserving age assurance. The Central Government should also consider using its power under Section 9(5) of the DPDP Act to provide graded protection for older adolescents, so that the consent requirement does not exclude them from beneficial services.
5. **Build enforcement capacity:** The Ministry of Home Affairs, through the Indian Cyber Crime Coordination Centre, and the State police forces should establish specialised child cybercrime units with trained investigators and forensic experts competent to certify electronic records under Section 63 of the BSA.
6. **Prefer targeted amendment to a new statute:** A dedicated online child-safety statute would offer coherence, but it would duplicate offences already found in the POCSO Act, the IT Act and the BNS and create new conflicts of interpretation. Targeted amendments to these statutes, supported by the intermediary rules, would close the identified gaps more quickly. The United Kingdom's approach is instructive: it addressed AI-generated abuse material by inserting new offences

into its existing sexual offences legislation rather than by enacting a separate code[79].

Future researchers may examine the practical effectiveness of the framework through empirical studies involving children, parents, teachers and law enforcement agencies, and may compare the approaches of other jurisdictions to online grooming and AI-enabled threats.

VI. CONCLUSION

This study asked whether the existing Indian legal framework adequately protects children from existing and emerging cybercrimes while safeguarding their rights and best interests in cyberspace. It finds that India has substantial legal mechanisms. The IT Act addresses identity theft, cheating by personation, privacy violations, sexually explicit material involving children and the online inducement of children. The POCSO Act addresses sexual offences and recognises their commission through electronic means, and the BNSS and BSA govern the collection and proof of electronic evidence. The intermediary rules impose duties on platforms, and the DPDP Act will regulate the processing of children's personal data from May 2027.

The framework is, however, fragmented, and it contains specific gaps: the absence of definitions of grooming and cyberbullying, uncertainty over wholly synthetic CSEAM, limited reach over foreign platforms and AI-model providers, the deferred commencement of the children's data safeguards and weak forensic capacity. These gaps call for targeted amendment and stronger enforcement rather than a new legal regime.

Children's rights in the digital environment extend beyond criminal protection to privacy, information and participation. General Comment No. 25 asks States to adopt a rights-based approach that keeps the best interests of the child at the centre, and Indian law should develop in that spirit.

[79] Crime and Policing Act 2026, c. 20, § 72 (UK).

VII. BIBLIOGRAPHY

A. Statutes, Rules and Orders (India)

1. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, Acts of Parliament, 2023 (India).
2. Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India).
3. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Acts of Parliament, 2023 (India).
4. Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
5. Digital Personal Data Protection (Removal of Difficulties) Order, 2026, S.O. 5458(E) (Oct. 5, 2026) (India).
6. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India).
7. Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
8. Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2009 (India).
9. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).
10. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India).
11. Protection of Children from Sexual Offences Act, No. 32 of 2012, Acts of Parliament, 2012 (India).
12. Protection of Children from Sexual Offences (Amendment) Act, No. 25 of 2019, Acts of Parliament, 2019 (India).

B. Cases

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
3. *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716 (India).
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

5. *Pune Bar Ass'n v. Union of India*, W.P. (C) No. 599 of 2026, 2026 LiveLaw (SC) 551 (India) (order dated May 22, 2026).
6. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

C. International Instruments and Foreign Legislation

1. Comm. on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).
2. Crime and Policing Act 2026, c. 20 (UK).

D. Journal Articles and Working Papers

1. Rahul Kailas Bharati, *Identity Theft and Impersonation in Cyberspace (Sections 66C and 66D of the IT Act, 2000)* (July 24, 2025) (working paper), https://ssrn.com/abstract=5379783.
2. Aratrika Choudhuri, *Conceptualising Children's Rights in Digital Spaces: Emerging Issues and Challenges*, 15 Socio-Legal Rev. 151 (2019), https://doi.org/10.55496/NTPF6562.
3. Ranjana Ferrao, *Special Courts for Children: Lessons Learnt from India*, 15 Int'l J. Ct. Admin., no. 2, 2024, art. 7, https://iacajournal.org/articles/10.36745/ijca.485.
4. 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., no. 1, 2025, at 1, https://doi.org/10.55496/SZWH4909.
5. Sumedha Gupta, *Child's Right in Cyberspace: A Critical Analysis of Protection and Privacy under the Indian Legal System*, 4 Int'l J. Legal Sci. & Innovation 148 (2022).
6. Naveen Kumar & Madhusmita Ronghangpi, *Cyber-bullying of Children: Impacts and Deterrent Measures in India*, 5 Indian J. Educ. Tech. 134 (2023), https://journals.ncert.gov.in/IJET/article/view/420.

7. Daniel Manoj et al., *Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation*, 4 Child Prot. & Prac. 100088 (2025).
8. Rita Ozoemena, *General Comment No. 25 on Children's Rights in Relation to the Digital Environment: Implications for Children's Right to Privacy and Data Protection in Africa*, 24 Hum. Rts. L. Rev. ngae018 (2024).
9. Ch. Rajender Reddy & Srinivas M., *Cybercrime Against Women in India: Closing the Consent, Evidence and Enforcement Gaps*, 9 Int'l J.L. Mgmt. & Human. 301 (2026), https://doi.org/10.63108/IJLMH.12835.
10. Ankit Sourav Sahoo, *The Legal Lacunae in Protecting Children from Cyber-Bullying and Grooming in India*, 4 J. Advance & Future Rsch. 120 (2026), https://rjwave.org/jaafr/papers/JAAFR2603615.pdf.
11. S. Shukla et al., *Legal Complexities of Adolescent Relationships: A Study of Protection of Child Sexual Offense Cases in India*, 16 Cureus e60475 (2024).
12. Nazuk Sood, *Data Protection Vis-à-Vis Right to Privacy*, 12 Int'l J. Rsch. & Sci. Innovation 1925 (2025).
13. Shivani Verma, *A Psycho-Legal Analysis of Cyber Behaviours of Children: Legal Responses to Online Delinquencies*, 8 Indian J. Educ. Tech. 225 (2026), https://journals.ncert.gov.in/IJET/article/view/1778.
14. S. Wefers et al., *Understanding and Deterring Online Child Grooming: A Qualitative Study*, 19 Sex Offending, art. e13147 (2024).
15. Anurag Yadav & Kaur, *Confronting the Growing Threat of Child Identity Theft in the Age of Digitalisation* (2024).
16. Divya Yadav, *Cyberbullying Laws in India: Current Challenges and Reforms*, 2 Int'l J. Legal Rsch. & Analysis, no. 7, Mar. 2025, at 23.

E. Books, Chapters and Dissertations

1. Shruthi Sarang S. Kamath, *Right to Privacy: Pre- and Post-Puttaswamy Developments*, *in* Emerging Trends in Constitutional Law and Human Rights Jurisprudence (Notion Press 2026).
2. Navonita Mallick et al., *Children's Data Protection in Smart Educational Platforms: Addressing Privacy Risks in Intelligent Communication Systems*, *in* Proceedings of the AI Summit 294 (2025).
3. Lina Acca Mathew, *Legislative Models of Prosecuting Child Sexual Abuse in India: A Review and Critical Analysis* (July 2017) (Ph.D. dissertation, Queensland University of Technology), https://doi.org/10.5204/thesis.eprints.107784.
4. S. Sarkar, *The Silent Victims of Cyber Space: Analyzing Cyber-Crimes Against Children in the Indian Context* (2026) (unpublished LL.M. dissertation, Kazi Nazrul University).
5. Vijeta Verma, Priyanshu Kumar & Drashya Singhal, *Safeguarding Children's Rights in the Digital Age: A Critical Analysis of India's Cyber Laws*, *in* Child Protection Laws and Crime in the Digital Era ch. 11 (Romil Rawat ed., 2025), https://doi.org/10.4018/979-8-3373-5132-2.ch011.

F. Official Reports and Online Sources

1. P. Rahul Ambedkar, *Protection of Children from Sexual Offences Act, 2012: An Overview*, Kerala Judicial Academy (Sept. 2024), https://cdnbbsr.s3waas.gov.in/s3ec030b6ace9e8971cf36f1782aa982a7/uploads/2024/09/2024092050.pdf.
2. Efua Andoh, *What You Need to Know Before Sharing Your Child's Life Online*, Monitor on Psych., June 2026, at 24, https://www.apa.org/monitor/2026/06/parents-children-sharing-online.
3. Child Exploitation and Online Protection Command, *What Is Online Child Sexual Abuse and Exploitation?* CEOP Safety Centre, https://ceop.police.uk (last visited Sept. 30, 2026).

4. *Cyber Crime Offences in the Domain of Bharatiya Nyaya Sanhita (BNS), 2023*, Indian Railways, https://ncr.indianrailways.gov.in/uploads/files/1749022724173-CYBER%20OFFENCES%20(BNS).pdf (last visited Oct. 25, 2026).
5. Milford D'Souza, *Understanding Cyber Crime Against Children: What You Need to Know*, CRY (Dec. 29, 2025), https://www.cry.org/blog/cyber-crime-against-children/.
6. DTE Staff, *Over 1,800 Cases of Cybercrimes Against Children Registered in 2022, Higher Than Last Year: NCRB*, Down To Earth (Dec. 6, 2023), https://www.downtoearth.org.in/governance/over-1-800-cases-of-cybercrimes-against-children-registered-in-2022-higher-than-last-year-ncrb-93236.
7. *1,87,702 Cases of Crimes Against Children Recorded in 2024: NCRB Data*, Deccan Herald (2026), https://www.deccanherald.com/india/187702-cases-of-crimes-against-children-recorded-in-2024-ncrb-data-3995822.
8. *Govt Held First Public Consultation on Proposed Digital India Act*, ThePrint (Mar. 10, 2023), https://theprint.in/economy/govt-held-first-public-consultation-on-proposed-digital-india-act/1432385.
9. K. Jaishankar & T. Divya, *Cyber Offences under the Information Technology Act*, e-PG Pathshala, https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/S001608/P001742/M022125/ET/1504245749E-Text-ITAct-JaishankarDivya.pdf.
10. National Commission for Protection of Child Rights, *Cyber Safety Guideline*, https://ncpcr.gov.in/public/index.php/viewPdf/16613369326305fd6444e1b_cyber-safety-guidline.pdf (last visited Oct. 25, 2026).
11. National Crime Records Bureau, Ministry of Home Affairs, *Crime in India 2024* (2026).
12. National Cybercrime Reporting Portal, *Learn About Cybercrime*, Ministry of Home Affairs, https://cybercrime.gov.in/webform/crimecatdes.aspx (last visited Sept. 30, 2026).

13. Gaurav Saluja, *Critical Assessment of Information Technology Act, 2000*, Legal Serv. India (Apr. 29, 2023), https://www.researchgate.net/publication/370375309_Critical_Assessment_of_Information_Technology_Act_2000.
14. Sadhna Singh, *Online Safety for Children: Protecting the Next Generation from Harm*, NITI Aayog (June 2025), https://www.niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf.
15. Shreya Suri & Vikram Jeet Singh, *Processing of Children's Personal Data under the DPDP Act: What Does It Mean for Businesses?*, ELP Law (Aug. 23, 2024), https://elplaw.in/leadership/processing-of-childrens-personal-data-under-the-dpdp-act-what-does-it-means-for-businesses-3/.
16. Tamil Nadu State Judicial Academy, *Protection of Children from Sexual Offences Act, 2012*, https://www.tnsja.tn.gov.in/article/pocso_material.pdf.
17. UNICEF, *Cyberbullying: What Is It and How to Stop It* (Jan. 2026), https://www.unicef.org/stories/how-to-stop-cyberbullying.
18. United Nations Office on Drugs and Crime, *Module 12: Interpersonal Cybercrime: Online Child Sexual Exploitation and Abuse*, https://sherloc.unodc.org/cld/pt/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html (last visited Oct. 3, 2026).