

The Effectiveness of the Pocso Act and the JJ Act in Addressing Cybercrimes Against Children

Saumetra Singh¹, Dr. Mirza Juned Beg²

¹Research Scholar, Law, Integral University, Lucknow

²Professor, Law, Integral University, Lucknow

Abstract

Children's vulnerability to online sexual exploitation and abuse has increased dramatically as a result of India's digital transition. The two major legislations that cover child protection are the Juvenile Justice (Care and Protection of Children) Act of 2015 and the Protection of Children from Sexual Offences (POCSO) Act of 2012. The efficacy of these laws in combating cybercrimes against children is critically assessed in this essay. The Juvenile Justice Act operates on essentially different rehabilitative premises that offer limited utility for cybercrime prevention, while POCSO has strong substantive provisions for prosecuting online sexual offenses against children, greatly strengthened by the Supreme Court's 2024 ruling in *Just Rights for Children Alliance v. S. Harish*, according to the paper's doctrinal analysis of statutory provisions, judicial pronouncements, and empirical data from the National Crime Records Bureau (NCRB). The central finding is that legislative adequacy has not translated into enforcement effectiveness: mandatory reporting obligations remain systematically unmet, intermediary accountability is inadequately operationalised, and child-friendly procedural safeguards exist more on paper than in practice. The paper concludes that India's child protection framework requires a paradigm shift from reactive penalisation to proactive digital governance, encompassing platform regulation, digital literacy, and specialised cyber-forensic infrastructure.

Keywords: POCSO Act, Juvenile Justice Act, cybercrimes against children, CSEAM, digital child protection, intermediary liability

I. Introduction

The type and scope of crimes against children have significantly changed as a result of the widespread use of digital technology in Indian culture. Once a privilege of physical places it is now available to children on minimally supervised mobile devices, including smartphones, tablets and computers, where they experience digital interaction with very little awareness of the risks they encounter. The National Crime Records Bureau (NCRB) reported 887 crimes against children in Jammu and Kashmir alone during 2024, with POCSO cases constituting 308 of these over one-third of the total.³ Across India, cybercrimes against children though constituting a relatively small proportion of total recorded offences

¹ Research Scholar, Faculty of Law, Integral University, Lucknow. (MCN : IU/R&D/2026-MCN0005050)

² Faculty of Law, Integral University, Lucknow.

³ "Cyberbullying can be as traumatic as physical abuse"; Delhi HC upholds POCSO conviction, SCC Online Blog, Aug. 5, 2025

present a disproportionately serious challenge due to their transnational character, the permanence of digital evidence, and the systematic underreporting that characterises online abuse.

India's legislative response to child sexual abuse has been anchored in two principal statutes. The Protection of Children from Sexual Offences Act, 2012 (POCSO), enacted to fulfil India's obligations under the United Nations Convention on the Rights of the Child, established a comprehensive framework of gender-neutral offences, child-friendly procedures, and graded punishments.⁴ The J.J. Act, 2015, replaced its 2000 predecessor with a rehabilitative orientation that treats children in conflict with law through a welfare-based rather than punitive lens. Together, these statutes are intended to address the full spectrum of child protection concerns, from sexual exploitation to juvenile delinquency.

The critical question animating this paper is whether these legislative instruments are effective in addressing cybercrimes against children. This question has acquired renewed urgency following the Supreme Court's landmark judgment in *Just Rights for Children Alliance v. S. Harish* (2024), which reversed a Madras High Court ruling that had held mere downloading or viewing of child pornography to be outside the ambit of POCSO.⁵ In addition to correcting a serious interpretive error, the Supreme Court's ruling imposed extensive obligations on social media intermediaries, ruling that they are not exempt from liability under Section 79 of the Information Technology Act unless they adhere to POCSO's reporting requirements.

This paper proceeds in five parts. Part II examines the statutory architecture of POCSO, focusing on its digital provisions. Part III analyses the Juvenile Justice Act's treatment of cyber offences and its structural limitations in this domain. Part IV evaluates enforcement effectiveness through the lenses of reporting mechanisms, intermediary accountability, and procedural safeguards. Part V concludes with recommendations for a preventive governance framework.

II. The POCSO Act and Cybercrimes Against Children

A. Substantive Provisions on Digital Offences

The POCSO Act, 2012, was drafted with an awareness that child sexual abuse increasingly occurs through electronic means. Section 12 punishes sexual harassment of a child as defined under Section 11, which explicitly encompasses conduct through electronic or online means, including making sexually coloured remarks, showing pornographic material, or repeatedly contacting a child with sexual intent⁶. The use of a child for pornographic purposes in any media electronic, printed, or broadcast for the goal of sexual enjoyment is illegal under Section 13.

For the first offense, Section 14 stipulates a minimum sentence of five years in jail and a fine. For a second or subsequent conviction, the punishment increases to imprisonment for not less than seven years along with fine.⁷ Section 15 lays out a graded punishment framework for storing or possessing

⁴ National Crime Records Bureau, Crime in India 2024, Chapter 4A — Crime Against Children (States & UTs) (Ministry of Home Affairs, 2025), as reported in "887 crimes against children reported in J&K in 2024," The News Now, May 7, 2026

⁵ *Just Rights for Children Alliance v. S. Harish*, Criminal Appeal Nos. 2161-2162 of 2024, ¶¶ 255-258 (Supreme Court of India, Sept. 23, 2024), <https://indiankanoon.org/doc/37078038/>

⁶ Ministry of Women and Child Development, Government of India, POCSO Act, 2012 provides for safeguarding children against sexual offences, including online sexual abuse, Press Information Bureau (Mar. 24, 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2245026>

⁷ Ministry of Women and Child Development, Government of India, POCSO Act, 2012 provides for safeguarding children against sexual offences, including online sexual abuse, Press Information Bureau (Mar. 24, 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2245026>

pornographic material involving children, including failure to delete, destroy, or report such material, depending upon the nature and purpose of the offence.⁸

These provisions are supplemented by the Information Technology Act of 2000. Publishing or transmitting content in electronic form that shows youngsters engaging in sexually explicit behavior is expressly prohibited by Section 67B. In addition to reporting offenses under POCSO, intermediaries are required by Rule 11 of the Protection of Children from Sexual Offences Rules, 2020 to provide the Special Juvenile Police Unit, the local police, or the cyber-crime portal with the relevant material, including the source from which it may have originated.

B. The 2024 Supreme Court Judgment: Closing the Impunity Gap

The Madras High Court's 2024 decision that merely downloading and watching child pornography did not constitute an offense under the Act put the efficacy of POCSO's digital provisions to the test. A chargesheet for offenses under Section 67B of the IT Act and Section 15(1) of POCSO was overturned by the High Court. The chargesheet was the result of a FIR that was filed after the accused was identified as an active consumer of child pornography in the NCRB's Cyber Tipline Report.

The Supreme Court's September 2024 judgment reversed this interpretive error with considerable force. The Court ruled that under POCSO and the IT Act, it is illegal to view, download, save, possess, distribute, or show pornographic activities involving children. The judgment evolved the doctrine of "constructive possession" to address evasion tactics, holding that a person is accountable if they possessed an "invariable degree of power and knowledge to control, manipulate, alter, modify or destroy the material".⁹

Crucially, the Court addressed the gap in intermediary accountability. It stated that social media intermediaries only follow the guidelines outlined in a Memorandum of Understanding with the National Center for Missing & Exploited Children (NCMEC), a US-based NGO, rather than reporting cases of child abuse and exploitation to the local authorities designated under POCSO. The Court held that an intermediary cannot claim exemption from liability under Section 79 of the IT Act unless due diligence is conducted, and that such due diligence includes not only removal of child pornographic content but also making an immediate report of such content to the concerned police units in the manner specified under POCSO.¹⁰

The Court additionally found that, to the extent of any conflict, the Act supersedes existing laws under Section 42A of POCSO. Therefore, an intermediary will not be released from any liability under POCSO simply because it complies with the requirements outlined in Section 79 of the IT Act unless it also complies with the requirements and procedure outlined under it, specifically Section 20 of POCSO and Rule 11 of the POCSO Rules.

C. The Delhi High Court's Cyberbullying Jurisprudence

Beyond pornography offences, POCSO's provisions on sexual harassment have been applied to cyberbullying involving sexual content. In a 2025 judgment, the Delhi High Court upheld a conviction where the accused had morphed a minor girl's face onto a nude body and sent the image to her via WhatsApp, accompanied by threats to circulate it further. The Court found that the morphed photograph

⁸ Just Rights for Children Alliance, ¶¶ 2-5 (describing charges under Sect. 67B of the IT Act and Sect. 15(1) of POCSO arising from NCRB Cyber Tipline Report)

⁹ Just Rights for Children Alliance v. S. Harish, Criminal Appeal Nos. 2161-2162 of 2024, ¶¶ 255-258 (Supreme Court of India, Sept. 23, 2024), <https://indiankanoon.org/doc/37078038/>

¹⁰ See Sect. 20 and Sect. 42A, Protection of Children from Sexual Offences Act, 2012 (POCSO Act), read with Rule 11 of the Protection of Children from Sexual Offences Rules, 2020; Sect. 79, Information Technology Act, 2000.

constituted “sexually explicit representation of a child” under Sections 11 and 13 of POCSO, and that the repeated threatening messages constituted stalking under Section 354D of the Indian Penal Code.¹¹ The Court observed that “cyberbullying can be as mentally traumatic and scarring as physical violence, especially when directed towards children.” It emphasised that “creating a safe environment for children cannot be restricted to physical spaces alone” and that “equal protection be extended to digital spaces.”

III. The Juvenile Justice Act and Cyber Offences

A. Structural Orientation: Rehabilitation Over Deterrence

POCSO and the Juvenile Justice (Care and Protection of Children) Act, 2015 are based on essentially distinct principles. The JJ Act is a welfare-oriented law that prioritizes the rehabilitation and social reintegration of children in conflict with the law, whereas POCSO is a criminal statute intended to pursue and punish perpetrators. The Act establishes Juvenile Justice Boards with jurisdiction over children alleged to have committed offences, prescribes inquiry procedures that are non-adversarial in character, and mandates that the child’s best interests guide all decisions.

This rehabilitative orientation, while consonant with international standards and constitutional values, creates structural limitations for addressing cybercrimes. The JJ Act was not designed with digital offences in mind. Its provisions for children in conflict with law focus on conventional juvenile delinquency theft, assault, and other traditional offences rather than the technologically sophisticated conduct that characterises cybercrimes. A child who creates and distributes AI-generated child sexual abuse material, for instance, does not fit neatly into the categories of offenders the JJ Act was designed to address.

B. Children as Victims of Cybercrimes

The JJ Act does contain provisions for “children in need of care and protection,” which could in principle encompass child victims of cybercrimes. According to Section 2(14), a kid is defined as one who is discovered working in violation of labor regulations, abused or neglected, or without a home or permanent place of residence. The Act establishes Child Welfare Committees to handle these cases, with procedures for inquiry, restoration to family, and placement in institutional care.

However, the JJ Act’s framework for children in need of care and protection is poorly adapted to the specific harms of cybercrimes. A child whose morphed images are circulating on social media, or who has been groomed online by a predator, does not necessarily meet the statutory definition of a child “in need of care and protection” in the conventional sense. The Act’s mechanisms production before the Child Welfare Committee, social investigation reports, placement in children’s homes are designed for children who are abandoned, orphaned, or subjected to physical abuse or exploitation, not for the digital-age harms of image-based abuse and online grooming.

C. The Absence of Cyber-Specific Provisions

Most significantly, the JJ Act contains no provisions that specifically address cyber offences, either by children or against them. There is no equivalent to POCSO’s Section 12 or 13, no mechanism for compelling intermediaries to remove harmful content involving a child in need of care and protection,

¹¹ See Protection of Children from Sexual Offences Act, 2012, §§ 11, 13; Indian Penal Code, 1860, § 354D (stalking); and the relevant 2025 judgment of the Delhi High Court concerning the morphed image of a minor circulated through WhatsApp.

and no framework for the digital rehabilitation of children whose abuse has been recorded and circulated online.¹²

The absence of such provisions creates a gap in the protective framework. While POCSO addresses the offence and punishes the offender, it does not comprehensively address the ongoing needs of the child victim the removal of content, the restoration of digital privacy, and the therapeutic interventions necessary to address the psychological trauma of knowing one's abuse is permanently accessible online. The JJ Act, with its welfare orientation, would be the logical instrument for addressing these needs, but it lacks the specific mechanisms to do so.

IV. Evaluating Enforcement Effectiveness

A. The Mandatory Reporting Deficit

The reporting of offenses is essential to POCSO's success. Anyone with information or suspicion of an offense is required by Section 19 to notify the local police or the Special Juvenile Police Unit. Failure to report is punishable under Section 21 by a fine and up to six months (or a year in some circumstances) in jail. The Act also imposes a duty on media personnel and studio personnel who come across such material in the course of their work to report it to the police.¹³

In practice, however, reporting under POCSO remains woefully inadequate. The underreporting of cybercrimes against children is driven by several factors. Social stigma and cultural taboos deter children and families from reporting online sexual exploitation. Digital illiteracy means that many children, parents, and even teachers are unaware of the mechanisms for reporting and the rights that POCSO protects. The complexity of online abuse the anonymity of offenders, the use of encrypted platforms, the transnational hosting of content further discourages reporting by creating an appearance of futility.

B. Intermediary Accountability: Between Mandate and Implementation

The 2024 Supreme Court judgment directed that social media intermediaries must report CSEAM to local police and authorities. Rule 11 of the POCSO Rules, 2020, already imposes due diligence obligations on intermediaries to prevent the hosting of harmful content. Yet the operationalisation of these obligations remains inadequate. In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act as unconstitutional for vagueness and overbreadth, holding that it violated Articles 19(1)(a) and 21 of the Constitution.¹⁴ While that judgment concerned a different provision, it affirmed the principle that state regulation of online content must be precise and narrowly tailored.

The Supreme Court in *Just Rights for Children Alliance* specifically addressed the gap between mandate and implementation. The Court noted that “social media intermediaries do not report such cases of child abuse and exploitation to the local authorities specified under POCSO and rather only comply with the requirements stipulated in the MOU” with the National Centre for Missing & Exploited Children. The Court held that “an intermediary cannot claim exemption from the liability under Section 79 of the IT Act for any third-party information, data, or communication link made available or hosted by it, unless

¹² JJ (Care and Protection of Children) Act, 2015; Protection of Children from Sexual Offences Act, 2012, §§ 12, 13; Protection of Children from Sexual Offences Rules, 2020.

¹³ Protection of Children from Sexual Offences Act, 2012, §§ 19, 20 and 21 (providing for mandatory reporting of offences, duties of media and other persons, and punishment for failure to report or record a case).

¹⁴ *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716; Protection of Children from Sexual Offences Rules, 2020, r. 11; Information Technology Act, 2000, § 79.

due diligence is conducted by it and compliance is made of these provisions of the POCSO”.¹⁵ The Court further clarified that “due diligence includes not only removal of child pornographic content but also making an immediate report of such content to the concerned police units in the manner specified under the POCSO Act and the Rules thereunder”.

Despite these clear judicial directions, the practical reality remains that CSEAM continues to be hosted and disseminated with ease. The gap between mandate and implementation reflects several factors. Intermediaries face no meaningful sanctions for non-compliance. The volume of content uploaded to platforms makes manual review impractical, and automated detection systems while improving remain imperfect. The transnational character of major platforms means that Indian law enforcement authorities face jurisdictional hurdles in seeking cooperation and accountability.

C. Child-Friendly Procedures: Promise and Performance

The procedural rules of POCSO are a major step forward for child-sensitive justice. According to Section 24, a child's statement must be recorded at their home or other preferred location, ideally by a female police officer. A parent or other trusted individual must be present for the medical examination, according to Section 27. According to Section 35, trials must be finished within a year, if at all possible, and evidence must be documented within thirty days. POCSO matters are heard in camera by Special Courts.¹⁶

The effectiveness of these provisions in the digital context is questionable. The delays that plague the Indian criminal justice system generally affect POCSO cases as well. The NCRB data for Jammu and Kashmir illustrates this: of 1,339 cases under investigation during 2024, 537 remained pending at year's end a pendency percentage of 40.1 per cent. In courts, 2,661 cases were pending trial or under court process, with only 12 convictions recorded during the year. For child victims of online abuse, whose images may continue to circulate while proceedings drag on, the delay is not merely an inconvenience but a continuing source of trauma.

D. Specialised Enforcement Deficit

The literature consistently identifies the shortage of specialised personnel and infrastructure as a critical constraint on enforcement effectiveness. Cybercrime investigation requires technical expertise in digital forensics, cryptocurrency tracing, and encrypted communication analysis skills that are in short supply in Indian police forces. Many police departments lack the necessary technology tools and knowledge to respond promptly to complex cybercrimes.¹⁷

The Supreme Court's judgment recognised this deficit in directing the establishment of a forensic lab equipped with cutting-edge technology to respond to CSEAM reports. Presently, international agencies like Interpol send Indian IP addresses to the NCRB which further relay the information to State Police for further action. Thus response time would be reduced if India had the ability to flag suspicious activity domestically in a domestic lab. The Court's direction represents a recognition that without specialised infrastructure, the legal framework's protections remain largely theoretical.

The Indian Cybercrime Coordination Centre (I4C) gives law enforcement organizations a framework to deal with cybercrimes in a planned and coordinated way. Cybercrimes that target vulnerable groups are

¹⁵ Just Rights for Children Alliance v. S. Harish, 2024 INSC 716 (Supreme Court of India), holding that due diligence under § 79 of the Information Technology Act includes removal of child sexual abuse material and immediate reporting to the concerned police authorities in accordance with the POCSO Act and Rules.

¹⁶ Protection of Children from Sexual Offences Act, 2012, §§ 24, 27, 35 and 37

¹⁷ Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C)

specifically addressed by the Cyber Crime Prevention Against Women and Children (CCPWC) program. Nonetheless, the challenge's scope continues to surpass the institutional response.¹⁸

V. The Path Forward: From Penal Legislation to Preventive Governance

A. Reframing Cybercrimes Against Children

The analysis suggests effectiveness of 'POCSO' and the JJ Act in addressing cybercrimes is constrained less by legislative inadequacy than by enforcement failure and conceptual limitations. 'POCSO' possesses robust substantive provisions, particularly as interpreted by the Supreme Court in 2024. The JJ Act, while structurally ill-suited to cybercrime, was not designed with these offences in mind. The critical gap is not in the law's text but in its translation into practice.

To be effective, the first step is conceptual: cybercrimes against children need to be seen as a systemic problem and systemic responses are needed. The 2024 Supreme Court judgment's engagement with the terminology of "child pornography" and its recognition that consumption of such material is participation in the exploitation of children has implications for enforcement priorities, for intermediary obligations, and for the treatment of victims.¹⁹

B. Operationalising Intermediary Accountability

The most significant gap in the current framework is the effective regulation of intermediaries. The Supreme Court's direction that intermediaries report CSEAM in real-time to law enforcement requires operationalisation through clear standards, meaningful penalties for non-compliance, and robust monitoring mechanisms. It's obvious from the Court's holding that the compliance with the NCMEC MOU is insufficient and that the intermediaries should report directly to the authorities of the Indian country under the 'POCSO' would provide the lawmakers a clear roadmap to follow.²⁰

A domestic forensic lab, set up by the Supreme Court, would boost India's ability to detect and react to CSEAM without depending on international referrals. This Infrastructure would also facilitate India's contribution towards global efforts to combat CSEAM by identifying content on other platforms and providing intelligence to international partners.

C. Strengthening Reporting and Victim Support

The mandatory reporting provisions of 'POCSO' require more effective implementation. The National Cyber Crime Reporting Portal (www.cybercrime.gov.in) enables citizens to report complaints relating to various categories of cybercrime, with a special focus on offences targeting women and children.²¹ This portal must be integrated with state-level cyber crime units to ensure that complaints are routed to the appropriate authorities and that their progress is tracked. Scattering district-level cyber cells equipped with trained staff and up-to-date gear would help overcome this enforcement obstacle.

The framework should go beyond reporting and instead focus on the continuing needs of child victims. The removal of CSEAM from platforms is essential but insufficient; children whose abuse has been recorded require therapeutic support, digital privacy protection, and assistance in navigating the psychological consequences of knowing their images may persist online. The JJ Act's welfare provisions could be amended to include specific provisions for child victims of cybercrimes, including mechanisms for content removal, identity protection, and rehabilitation services.

¹⁸ Ministry of Home Affairs, Government of India, Cyber Crime Prevention Against Women and Children (CCPWC) Scheme

¹⁹ Just Rights for Children Alliance & Anr. v. S. Harish & Ors., 2024 INSC 716

²⁰ Just Rights for Children Alliance & Anr. v. S. Harish & Ors., 2024 INSC 716

²¹ National Cyber Crime Reporting Portal, Government of India

D. Digital Literacy and Prevention

The most effective long-term strategy for addressing cybercrimes against children is prevention through digital literacy. The NCRB data always highlights the issue of lack of awareness among children, parents and teachers as a critical vulnerability. School curricula enhancements, parent and teacher training on cyber safety issues and public awareness campaigns are critical to complement legal enforcement.

Together with the Ministry of Electronics and Information Technology and the Ministry of Home Affairs, the Ministry of Women and Child Development, has developed a comprehensive institutional framework for preventing, detecting, and addressing online child sexual abuse and exploitation. This framework must be implemented with adequate resources and monitored for effectiveness. Prevention should not only focus on potential victims, but also potential offenders, and focus on the demand-side dynamics that the Supreme Court identified as fueling the cycle of exploitation.

E. International Cooperation

The transnational character of cybercrimes against children requires international cooperation that current mutual legal assistance treaty mechanisms are ill-equipped to provide. The delays and complexities of MLAT procedures enable offenders to destroy evidence or evade prosecution. The Supreme Court's recognition of the NCMEC-NCRB reporting mechanism highlights the importance of international coordination, but also reveals its limitations when intermediaries treat such reporting as sufficient compliance with domestic law. An international database of sexual offenders, coordinated financial tracking to disrupt the money trails that sustain CSEAM networks, and streamlined mechanisms for cross-border evidence sharing would significantly enhance enforcement effectiveness.

VI. Conclusion

In the modern world, one of the main trends is the use of various technologies by companies of different sizes. In this regard, it should be noted that organizations that implement artificial intelligence in their work processes gain a considerable amount of advantages. These technological solutions allow for optimizing many monotonous and routine aspects of business operations. As a result, companies reduce costs due to the automation of business processes. Nevertheless, it should be emphasized that technology alone is not enough for business success. Businesses need to stimulate and motivate employees to innovate and effectively use new advanced solutions.

Central finding of this paper is that legislative adequacy is a necessary but not sufficient condition for effectiveness. The gap between law and practice manifested in the failure to report offences, the inadequacy of intermediary accountability, the shortage of specialised enforcement capacity, and the delays in judicial proceedings renders POCSO's protections largely theoretical for many child victims. The Supreme Court's 2024 judgment represents a significant judicial intervention, but judicial directives cannot substitute for administrative capacity and political will.

The path forward requires a paradigm shift from reactive penalisation to preventive governance. This entails operationalising intermediary accountability through meaningful penalties and monitoring, building specialised cyber-forensic infrastructure, strengthening reporting mechanisms and victim support services, investing in digital literacy and prevention, and pursuing international cooperation against the transnational networks that sustain CSEAM. Only through such a comprehensive approach one that addresses the ecosystem of digital child exploitation rather than merely its individual manifestations can India's legal framework fulfil its promise of protecting children in the digital age.

References

1. The Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code (2012), <https://www.indiacode.nic.in/handle/123456789/12903>.
2. Protection of Children from Sexual Offences Rules, 2020, Rule 11 (India), <https://indiankanoon.org/doc/3021296/>.
3. Information Technology Act, No. 21 of 2000, § 67B (India).
4. *Just Rights for Children Alliance v. S. Harish*, Criminal Appeal Nos. 2161-2162 of 2024 (Supreme Court of India, Sept. 23, 2024), <https://indiankanoon.org/doc/37078038/>.
5. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (Supreme Court of India).
6. *State (NCT of Delhi) v. [Accused]*, 2025 SCC OnLine Del 4821 (Delhi High Court, July 28, 2025).
7. Press Information Bureau, Government of India, 'POCSO' Act, 2012 provides for safeguarding children against sexual offences, including online sexual abuse (Mar. 24, 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2245026>.
8. Press Information Bureau, Government of India, *Comprehensive and coordinated institutional framework put in place to prevent, detect and combat online sexual abuse and exploitation of children* (Aug. 4, 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2294855>.
9. National Crime Records Bureau, *Crime in India 2024* (Ministry of Home Affairs, 2025), <https://www.ncrb.gov.in/crime-in-india.html>.
10. Child Rights and You (CRY), *Analysis of NCRB Data on Cybercrimes Against Children* (2026), as reported in *The Tribune*, *Nearly 9 in 10 cybercrimes against children involve sexually explicit content: NCRB data* (May 7, 2026), <https://www.tribuneindia.com/news/india/nearly-9-in-10-cybercrimes-against-children-involve-sexually-explicit-content-ncrb-data/>.
11. *Deccan Herald*, *1,87,702 cases of crimes against children recorded in 2024: NCRB data* (May 7, 2026), <https://www.deccanherald.com/india/187702-cases-of-crimes-against-children-recorded-in-2024-ncrb-data-3995822>.
12. SCC Online Blog, 'Cyberbullying can be as traumatic as physical abuse'; *Delhi HC upholds 'POCSO' conviction; Bats for safer digital spaces for children* (Aug. 5, 2025), <https://www.sconline.com/blog/post/2025/08/06/safer-digital-spaces-for-children-delhi-hc-pocso-cyberbullying-case/>.
13. Dhyeya Law, *Child Rights & Legal Protection: Just Rights for Children Alliance Case*, <https://www.dhyeyalaw.in/just-rights-for-children-alliance-v-s-harish>.
14. *Drishti Judiciary*, *Child Sexual Exploitative and Abuse Material* (Sept. 24, 2024), <https://www.drishtijudiciary.com/current-affairs/child-sexual-exploitative-and-abuse-material>.
15. IPRMENTLAW, *Compliance of 'POCSO' necessary for "Safe Harbour" protection for intermediaries* (Oct. 19, 2024), <https://iprmentlaw.com/2024/10/20/compliance-of-pocso-necessary-for-safe-harbour-protection-for-intermediaries/>.
16. United Nations Convention on the Rights of the Child, adopted Nov. 20, 1989, 1577 U.N.T.S. 3 (entered into force Sept. 2, 1990).
17. The Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016 (India Code, 2015).
18. Indian Cybercrime Coordination Centre (I4C), Ministry of Home Affairs, Government of India.
19. Cyber Crime Prevention Against Women and Children (CCPWC) Scheme, Ministry of Home Affairs, Government of India.

20. National Cyber Crime Reporting Portal, <https://www.cybercrime.gov.in>.