LAW

Child Victimology in the Age of Artificial Intelligence: A Critical Study of Deepfake Abuse, Online Exploitation and Emerging Cyber Threats

Vishoka Singh Thakur[1], Ravinderjeet Khattra[2]

[1]LL.M. Student, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India
[2]Assistant Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

Published November 2026

Abstract

Artificial intelligence has changed how online abuse is produced, circulated and concealed. Generative systems can create realistic sexualised depictions of children, convert ordinary photographs into fabricated intimate images, imitate voices, assist grooming and accelerate the circulation of exploitative material. These practices unsettle conventional accounts of victimisation. A child may suffer serious harm even when an image is synthetic, no physical contact has occurred and the child was never photographed in an abusive situation. Humiliation, threats, extortion, reputational injury and the loss of control over one's identity may persist long after the original content has been created. This paper examines child victimology in the context of artificial intelligence, focusing on deepfake abuse, online sexual exploitation and emerging cyber threats. It adopts a doctrinal and analytical method, drawing on Indian legislation, judicial developments and international child-rights standards. India's legal framework includes the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Their application to synthetic material, however, raises questions about statutory interpretation, proof, intermediary responsibility, timely removal and remedies suited to children. The Digital Personal Data Protection Act, 2023 also establishes a child-specific privacy framework, although the commencement of its provisions has been phased. The paper argues that a legal response cannot be measured by the existence of offences alone. Effective protection requires clarity about the reach of criminal law, prompt removal procedures that preserve evidence, proportionate duties for platforms and AI developers, specialised investigation and accessible support for affected children. Digital literacy and trauma-informed institutional practices must form part of the same framework. The use of new technology does not reduce the child's claim to dignity, privacy and an effective remedy.

Keywords: Child victimology; artificial intelligence; deepfakes; child sexual exploitation; cybercrime; POCSO; digital privacy; intermediary liability

1 Introduction

Childhood now unfolds, in significant part, through networked spaces. Education, recreation, communication and social participation increasingly depend on social media, messaging services, online games and other digital platforms. These spaces expand access to information and connection, but they also expose children to grooming, coercion, impersonation, sexual extortion, cyberbullying, privacy violations and the circulation of abusive material. Artificial intelligence changes the scale and character of these risks. It reduces the technical effort required to manipulate images and voices, while allowing harmful conduct to be repeated and distributed with little cost.

Deepfakes are synthetic or manipulated audio-visual materials produced or altered through machine-learning techniques. In cases involving children, an ordinary photograph may be transformed into a fabricated sexual image; a child's voice or likeness may be reproduced to create humiliating, deceptive or coercive content. Such material may circulate among classmates, be used to threaten the child or be distributed for financial or sexual gratification. Whether the material is genuine or synthetic remains relevant to legal classification. It does not, however, determine whether the child has been harmed.

Victimology examines the causes and consequences of victimisation, the relationship between victims and offenders, and the institutional response to injury. Child victimology adds considerations of developmental vulnerability, dependency, unequal power and the State's heightened duty of protection. A child whose likeness is inserted into a fabricated intimate image may experience consequences comparable to those faced by a child whose intimate image was recorded and shared without consent. The artificial origin of the image does not make the resulting fear, humiliation or coercion any less real.

The legal problem has two connected dimensions. The first concerns the extent to which existing laws cover abuse enabled by artificial intelligence. The second concerns whether institutions respond in ways that protect the child or deepen the original injury. This paper addresses those questions in the Indian context, informed by international child-rights principles [1].

2 Research objectives, questions and methodology

The study examines the forms of child victimisation enabled by artificial intelligence and assesses the adequacy of India's legal and institutional response. Its specific objectives are to: (i) explain the victimological dimensions of deepfake abuse; (ii) identify significant forms of AI-enabled online exploitation; (iii) analyse the relevant Indian statutes and judicial principles; (iv) examine enforcement and evidentiary gaps; and (v) propose a child-centred framework for prevention, investigation and redress.

Four questions guide the inquiry. How does artificial intelligence alter the scale, character and consequences of child victimisation? To what extent do the POCSO Act and the Information Technology Act address synthetic sexual material and associated conduct? What responsibilities should apply to online intermediaries and AI service providers? Finally, what safeguards are needed to ensure that reporting, investigation and adjudication do not expose children to further harm?

The research is doctrinal and analytical. It draws on primary legal materials, including statutes, rules and judicial decisions, and considers relevant international instruments and policy literature. It does not claim to measure the prevalence of AI-enabled abuse or establish statistical causation. The discussion is therefore a legal and policy assessment, not an empirical account of incidence. The law is stated as at November 13, 2026. Particular care is taken to distinguish provisions that are in force from those whose commencement has been deferred [2].

3 Child victimology and the best interests of the child

A child-centred account must recognise several connected forms of injury. Psychological consequences may include anxiety, shame, fear, depression and loss of trust. Social consequences may take the form of bullying, exclusion, reputational damage or interruption of education. A child's sexual and bodily autonomy is violated when their likeness is appropriated for sexualised material

without consent. Informational privacy is also compromised when photographs, personal details, location data or voice samples are extracted and misused. Institutional responses can create a further injury where authorities require repeated retelling, circulate sensitive evidence unnecessarily or imply that the child is responsible for the abuse.

The best-interests principle requires the child's safety and development to remain a primary consideration in decisions affecting them. That obligation must inform platform design, complaint procedures, police action, evidence management and court processes. A child should not be blamed for an offender's manipulation. Nor should synthetic material be treated as harmless simply because it does not record an actual sexual act.

Vulnerability must not be confused with an absence of agency. Children use technology in varied and increasingly sophisticated ways. Their participation and capacity to make choices should be respected through age-appropriate information and accessible reporting. At the same time, their developmental circumstances and unequal power in relation to adults, platforms and offenders require safeguards that cannot be left to individual children to provide for themselves.

4 Deepfake abuse and synthetic sexual material

Deepfake abuse involves the unauthorised creation or use of synthetic media to make a person appear to say or do something that did not occur. A photograph of a child taken from a public profile may, for example, be altered into a sexualised image. Face-swapping applications, image-generation systems and voice-cloning tools can make the resulting material appear credible to classmates, teachers or family members. It may then be used to humiliate, threaten, blackmail or isolate the child.

The harm lies not only in the image but also in the coercive conduct surrounding it. An offender may threaten publication unless the child supplies further photographs, pays money, enters a relationship or complies with other demands. Such conduct may amount to technology-facilitated sexual extortion. The threat can be experienced as real even where an adult observer recognises that the image has been manipulated. When the material reaches a school or local community, the consequences may be immediate: the child may face ridicule, suspicion, exclusion or pressure to explain an event that never occurred.

Synthetic material also raises a question of statutory construction. Does a provision referring to the use of a child for pornographic purposes, or to material depicting a child, extend to a wholly AI-generated image that resembles an identifiable child but records no actual act? The answer may turn on the statutory language, the extent to which the likeness identifies a real child, the accused person's conduct and the applicable mental elements. It would be unsafe to assume that every synthetic image automatically satisfies every element of an offence under the POCSO Act. Equally, the use of software rather than a camera should not, by itself, create an escape from accountability where the statutory ingredients are otherwise established.

A distinction may also arise between realistic depictions of identifiable children and wholly fictional, non-identifiable characters. Legislative clarification would reduce uncertainty, particularly in relation to images generated from a real child's face, voice or biometric features. Any definition should attend to identifiability, exploitation, intent, distribution and resulting harm. It should also be drafted with sufficient precision to protect bona fide artistic, scientific and educational expression [3].ONLINE EXPLOITATION AND EMERGING CYBER THREATS

AI-enabled exploitation extends beyond deepfake pornography. Chatbots can assist grooming by generating persuasive messages, adopting the language of a child's peers or sustaining conversations over time. Automated tools may help offenders identify children, tailor manipulation to their interests and communicate across languages. AI-generated profiles can impersonate classmates or trusted adults. Voice cloning may be used to fabricate an urgent request from a parent or relative; synthetic video can lend credibility to impersonation during live interactions.

The wider threat environment includes sextortion, doxxing, cyberstalking, non-consensual sharing of intimate material, malicious image editing, account takeover, data theft and targeted harassment. Recommendation systems and rapid-forwarding functions may increase the reach of abusive content. Encrypted services provide legitimate privacy protections, yet they can also complicate detection and the collection of evidence. The legal response must address that difficulty without treating unrestricted surveillance of children as an acceptable solution.

The accessibility of generative tools is compounded by the persistence of digital traces. A photograph may be extracted from an account, retained in datasets, copied into private groups and reused for later abuse. Removing it from one platform does not ensure that every copy has disappeared. Search results, caches, mirrors and repeated uploads can keep the material accessible. A takedown is therefore only one part of an effective remedy; it cannot, by itself, end the victimisation.

Artificial intelligence may also assist prevention. Detection systems can identify known abusive material, flag suspected synthetic manipulation, recognise grooming patterns and help prioritise complaints. These systems are not neutral or infallible. False positives may wrongly classify lawful material, while errors may fall disproportionately on particular groups. Human review, transparent standards, meaningful appeal procedures and independent oversight are necessary if automated detection is to protect children without producing new forms of harm.

5 Indian legal framework: POCSO and the IT Act

The Protection of Children from Sexual Offences Act, 2012 is India's principal child-specific criminal statute. It defines a child as a person below eighteen years and creates offences relating to sexual assault, sexual harassment and the use of children for pornographic purposes. Section 13 addresses the use of a child for pornographic purposes, including the representation of a child's sexual organs or the use of a child in real or simulated sexual acts. Sections 14 and 15 prescribe punishment for such use and address the storage of pornographic material involving a child, subject to the distinctions and conditions contained in the Act.

The statutory scheme recognises that exploitation may occur through representation and production, not only through physical contact. AI-generated material nevertheless tests the boundaries of the expressions "use of a child" and "representation of a child". Where an offender appropriates an actual child's face or likeness, the connection to the child is direct. Where the image is wholly synthetic and no real child is identifiable, the statutory position is less certain. Clarification would assist courts and investigators and reduce the risk of inconsistent application.

The Information Technology Act, 2000 operates alongside POCSO. Section 67B criminalises specified conduct involving electronic material depicting children in a sexually explicit, obscene or indecent manner. The provision addresses a broad range of conduct, including publishing, transmitting, creating, collecting, seeking, browsing, downloading, advertising, promoting, exchanging and distributing such material. It also addresses online enticement and the facilitation of child abuse. The

breadth of the provision matters in digital environments, where different actors may participate at separate stages of creation and circulation.

Other provisions of the IT Act may apply according to the facts, including those concerning privacy violations and sexually explicit electronic material. Their application must remain tied to the statutory ingredients and the evidence available. The presence of artificial intelligence does not, in itself, establish a separate offence. The prosecution must prove the conduct and mental elements required by the provision charged [4].

6 Indian legal framework: Intermediaries, data and general criminal law

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due-diligence obligations on intermediaries. Rule 3(1)(b) requires intermediaries to inform users that specified categories of unlawful or harmful information must not be hosted, displayed, uploaded, modified, published, transmitted, stored or shared. The listed categories include material harmful to children, sexually explicit or paedophilic content, invasion of privacy and impersonation. Under Rule 3(2)(b), an intermediary receiving a complaint from an individual, or a person acting on that individual's behalf, must take reasonable and practicable measures within twenty-four hours to remove or disable access to certain intimate or impersonating content, including artificially morphed images.

The rule offers a route for responding to deepfake abuse, but the existence of a complaint mechanism does not guarantee an effective remedy. Its practical value depends on whether a child or representative can report the material easily, identify the relevant URLs or accounts, secure preservation of evidence and obtain action against repeated uploads. A child should not have to interpret complex legal language or repeatedly submit intimate material to establish that abuse has occurred.

The Digital Personal Data Protection Act, 2023 provides for specific obligations in relation to children. Section 9 addresses verifiable parental consent, processing likely to cause detrimental effects on a child's well-being, and restrictions on tracking, behavioural monitoring and targeted advertising directed at children. Its operative status must, however, be stated accurately. The commencement notification dated November 13, 2025 phases the Act's provisions; sections 3 to 17, including section 9, are scheduled to commence eighteen months after publication. Accordingly, as at November 13, 2026, section 9 is not yet in force. Enactment and commencement are distinct legal events.

The Bharatiya Nyaya Sanhita, 2023 may apply to associated conduct depending on the circumstances. Provisions concerning sexual harassment, voyeurism, stalking, criminal intimidation, cheating and identity-related conduct may be relevant. Section 77, which addresses voyeurism, is framed around a woman engaged in a private act; it should not be treated as a general offence covering every form of deepfake abuse. The appropriate charge must follow the facts and the language enacted by Parliament. Extending a provision beyond its terms may weaken, rather than strengthen, the legal response [5].

7 Judicial approach and child-centred interpretation

In Just Rights for Children Alliance v. S. Harish, the Supreme Court of India considered the legal treatment of child sexual abuse material and addressed the seriousness of possession, viewing and circulation in the digital environment. The Court discussed the expression "child pornography" and

preferred the term "child sexual exploitative and abuse material" (CSEAM), recognising that the former may conceal the coercion and exploitation involved. The terminology matters to a victimological analysis: the material is not a neutral category of content but evidence of abuse involving a child.

The decision also requires attention to the different stages of digital exploitation, including creation, possession, viewing and dissemination. It should not, however, be treated as resolving every issue raised by wholly synthetic deepfakes. The relevant provisions of POCSO and the IT Act must still be applied to the facts and statutory elements of each case. The judgment supplies an important interpretive foundation for centring the child's dignity and protection, while the treatment of non-identifiable fictional imagery may require further judicial or legislative consideration.

Constitutional values support a child-centred approach. Article 21's protection of life, dignity, privacy and personal liberty informs the State's responsibility to protect children from serious digital harm. In K.S. Puttaswamy v. Union of India, the Supreme Court recognised privacy as a constitutionally protected right. A child's image, voice, identity and intimate data should not be treated as mere technical inputs. Their misuse can affect autonomy, reputation and psychological integrity.

A judicial process that protects children must do more than determine criminal liability. It should limit repeated testimony, protect identity, prevent unnecessary disclosure of intimate evidence and ensure access to appropriate support. The purpose of the process is not exhausted by conviction; it must also secure protection and reduce the harm caused by the proceedings themselves [6].

8 Critical gaps and implementation challenges

The first difficulty is definitional. Existing statutes were not drafted with contemporary generative systems in view. Broad statutory language may reach many forms of electronic exploitation, but uncertainty remains where synthetic material depicts an identifiable child without recording an actual sexual act. The law should clarify how realistic AI-generated depictions, face-swapped images, synthetic voices and derivative material are to be treated. That clarification must distinguish exploitative conduct from legitimate expression and remain consistent with the requirement of legal certainty.

The second difficulty concerns investigative capacity. Police personnel may not have adequate training in synthetic-media detection, cloud-based evidence, cryptocurrency-linked extortion or cross-border data requests. A manipulated image may be technically sophisticated, while the child's device preserves only fragments of the interaction. Investigators need access to forensic expertise and clear procedures for preserving metadata, hashes, URLs, timestamps and chain of custody. Such procedures must also prevent unnecessary duplication or circulation of abusive material.

Third, remedies offered by platforms remain fragmented. A complaint may be acknowledged by one service while copies continue to circulate elsewhere. Children and parents may not know whether to approach the platform, the police, the cybercrime portal or a child-protection authority. Coordinated referrals and a single, accessible reporting interface could reduce delay and uncertainty. Removal should be accompanied by lawful preservation of relevant evidence; otherwise, the steps taken to protect the child may inadvertently impair an investigation.

Fourth, the relationship between privacy and detection requires careful treatment. Blanket monitoring of children's communications can intrude upon privacy and discourage lawful expression. Automated scanning may generate false accusations or expose sensitive material to additional

reviewers. Monitoring measures must therefore satisfy standards of necessity and proportionality, operate transparently and remain subject to independent safeguards.

Finally, stigma continues to deter reporting. A child may fear punishment for using social media, sharing an image or communicating with an unknown person. Families and schools must not respond by assigning blame to the child. The relevant inquiry is the offender's coercion and misuse of technology, not the child's ordinary participation in digital life.

9 Recommendations

A coherent response to AI-enabled child exploitation must connect legal clarity with technical safeguards and victim support. The following measures address the principal gaps identified above.

1. **Clarify criminal-law coverage.** Parliament should expressly consider realistic synthetic sexual depictions of identifiable children, including material generated from a child's face, voice or other personal data. The law should define the relevant conduct and mental elements with precision, distinguish depictions of identifiable real children from wholly fictional material, and protect bona fide educational, scientific and artistic uses.
2. **Establish rapid, child-friendly reporting.** Platforms should provide a simple reporting route accessible to a child, parent, guardian or authorised support person. A report should lead to prompt risk assessment, removal or disabling of access where legally required, preservation of relevant evidence and communication of the outcome in language the child can understand. A child should never be required to upload the abusive material again as proof of the complaint [7].
3. **Adopt safety-by-design obligations.** AI developers and platforms should assess foreseeable risks before deployment, take reasonable steps to prevent unauthorised use of children's likenesses, restrict the generation of sexualised depictions of minors, maintain effective reporting channels and submit safety systems to regular independent audit. These measures must be proportionate; child protection should not become a justification for indiscriminate surveillance.
4. **Strengthen investigation.** Specialised cyber units require training in synthetic-media forensics, open-source intelligence, cloud preservation, cross-border cooperation and trauma-informed interviewing. Investigators should preserve original files and metadata securely, use cryptographic hashes where appropriate and restrict access to sensitive evidence. Standard procedures should protect both evidentiary integrity and the child's privacy.
5. **Provide integrated victim services.** Every reported case should be capable of referral to counselling, legal aid, child-welfare services and school-based support. Identity protection, safety planning and assistance with removal should be available without making support conditional on a criminal conviction.
6. **Improve digital literacy.** Schools should address privacy settings, consent, image-based abuse, grooming, impersonation and reporting. Parents should be encouraged to respond calmly and supportively when a child discloses abuse. Prevention cannot be placed solely on children; platforms, institutions and adults retain their own responsibilities.
7. **Ensure accountability and transparency.** Platforms should publish meaningful information about child-safety complaints, response times, repeat uploads and appeal outcomes, subject to privacy safeguards. Independent oversight should examine error rates, discriminatory effects and the actual performance of safety systems. Transparency is useful only when it enables scrutiny and leads to corrective action.

10 Conclusion

Artificial intelligence has changed the conditions in which children may be exploited online. Deepfake abuse makes clear that serious sexualised harm can occur even where the image is synthetic and no physical contact has taken place. The consequences may include coercion, humiliation, extortion, reputational injury and a continuing loss of control over identity. Child victimology must therefore recognise the digital image as a means through which dignity, privacy and autonomy can be violated.

India's legal framework already contains significant protections. POCSO addresses the use of children for pornographic purposes; section 67B of the Information Technology Act covers a wide range of electronic conduct involving sexually explicit or indecent material depicting children; and the 2021 Intermediary Rules provide due-diligence and rapid-removal mechanisms for specified harmful and impersonating content. The child-specific protections in the DPDP Act are also relevant, but their phased commencement must be acknowledged. The Supreme Court's decision in Just Rights for Children Alliance v. S. Harish strengthens the understanding that child sexual abuse material records exploitation and cannot be treated as neutral content.

The existence of legal provisions, however, does not by itself secure children's safety. Definitions must respond to synthetic media without sacrificing legal precision. Investigating agencies need technical competence and child-sensitive procedures. Platforms must act promptly, preserve evidence responsibly and provide accessible reporting. Children and families also require support that does not depend on the success of a prosecution. Prevention must combine safety-by-design, digital literacy, privacy safeguards and institutional accountability.

Technological novelty cannot become a defence for exploitation. A child's rights do not diminish because abuse is generated by a model, mediated by an algorithm or distributed through a platform. The law must respond to the substance of the harm while preserving precision, proportionality and due process. The adequacy of a protective framework should be judged not only by removals or prosecutions, but by whether children can participate in digital life without fear, stigma or preventable abuse [8].

References

[1] Convention on the Rights of the Child, 1989, arts. 3 and 19; UNICEF. *Artificial Intelligence and Child Sexual Abuse and Exploitation*. Issue brief, February 2026. https://www.unicef.org/reports/artificial-intelligence-and-child-sexual-abuse-and-exploitation

[2] Protection of Children from Sexual Offences Act, 2012, ss. 2 and 13–15; Digital Personal Data Protection Act, 2023, s. 1(2), read with G.S.R. 843(E), Ministry of Electronics and Information Technology (13 November 2025).

[3] Protection of Children from Sexual Offences Act, 2012, ss. 13–15; Information Technology Act, 2000, s. 67B; UNICEF. *Artificial Intelligence and Child Sexual Abuse and Exploitation*. Issue brief, February 2026. https://www.unicef.org/reports/artificial-intelligence-and-child-sexual-abuse-and-exploitation

[4] Protection of Children from Sexual Offences Act, 2012, ss. 2(1)(d), 13, 14 and 15; Information Technology Act, 2000, ss. 66E, 67, 67A and 67B.

[5] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1)(b) and 3(2)(b); Digital Personal Data Protection Act, 2023, s. 9; G.S.R. 843(E), Ministry of Electronics and Information Technology (13 November 2025); Bharatiya Nyaya Sanhita, 2023, ss. 75 and 77–79.

[6] Just Rights for Children Alliance v. S. Harish, 2024 INSC 716; K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; Protection of Children from Sexual Offences Act, 2012, ss. 33, 36 and 37.

[7] Information Technology Act, 2000, ss. 69A and 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3 and 4; Convention on the Rights of the Child, 1989, arts. 16 and 39.

[8] Just Rights for Children Alliance v. S. Harish, 2024 INSC 716; Convention on the Rights of the Child, 1989, arts. 3, 19, 34 and 39.