# INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 1 OF 2026

INSTITUTE OF LEGAL EDUCATION

# INDIAN JOURNAL OF LEGAL REVIEW

**APIS – 3920 – 0001 | ISSN - 2583-2344**

**(Open Access Journal)**

**Journal's Home Page – https://ijlr.iledu.in/**

**Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/**

**Volume 6 and Issue 1 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-1-of-2026/)**

**Publisher**

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in


INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# BEYOND PHYSICAL HARM: RETHINKING INDIA'S LEGISLATIVE FRAMEWORK TO ADDRESS DIGITAL SEXUAL ABUSE IN THE AGE OF ARTIFICIAL INTELLIGENCE

**AUTHOR –** SANDHYA PRABHAKARAN, LLM STUDENT AT AMITY INSTITUTE OF ADVANCED LEGAL STUDIES, AMITY UNIVERSITY UTTAR PRADESH

**BEST CITATION –** SANDHYA PRABHAKARAN, BEYOND PHYSICAL HARM: RETHINKING INDIA'S LEGISLATIVE FRAMEWORK TO ADDRESS DIGITAL SEXUAL ABUSE IN THE AGE OF ARTIFICIAL INTELLIGENCE, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (1) OF 2026, PG.1130-1137, APIS – 3920 – 0001 & ISSN – 2583-2344

## I. ABSTRACT

The rapid expansion of digital technologies has fundamentally altered the nature, scale, and impact of sexual harm. While traditional criminal law frameworks in India conceptualize sexual offences primarily through physical proximity and bodily violation, emerging forms of digital sexual abuse such as non-consensual dissemination of intimate images, deepfake pornography, sextortion, cyberstalking, morphing, and AI-generated sexual contentchallenge these assumptions. This paper examines the conceptual foundations of digital sexual abuse through international human rights norms relating to privacy, dignity, sexual autonomy, and gender equality, and critically evaluates the adequacy of the Indian legislative framework. Although statutes such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Protection of Children from Sexual Offences Act, 2012, and the Digital Personal Data Protection Act, 2023 address aspects of technology-facilitated harm, they operate in a fragmented and reactive manner. The absence of a consolidated statutory definition of digital sexual abuse, the lack of AI-specific offences, limited intermediary accountability, and inadequate victim-centric remedies expose significant normative and procedural gaps. Drawing upon constitutional jurisprudence on privacy and dignity, this paper argues for a comprehensive, consent-based legislative framework that recognizes digital sexual abuse as a distinct category of sexual violence. It proposes statutory reform integrating technological foresight, strengthened enforcement mechanisms, and rights-based safeguards to ensure protection of autonomy, identity, and dignity in the digital age.

***Keywords:*** *Digital Sexual Abuse; Non-Consensual Intimate Images; Deepfake Pornography; Sexual Autonomy; Informational Privacy; Artificial Intelligence; Cybercrime Law; Intermediary Liability; Victim-Centric Remedies; Constitutional Dignity.*

## II. INTRODUCTION

The advent of the modern internet traces its institutional origin to 1 January 1983, when ARPANET adopted the Transmission Control Protocol/Internet Protocol (TCP/IP), thereby creating a unified communication language for interconnected networks.[2534] This development laid the technological foundation of the contemporary digital ecosystem. Over the past four decades, the exponential growth of internet penetration has revolutionized commerce, governance, communication, and social interaction. Simultaneously, however, the same technological architecture has enabled the proliferation of cybercrime, including technology-facilitated sexual offences.

Digital platforms have rendered the commission of offences borderless, cost-efficient, and anonymous. Cybercrime today encompasses financial fraud, identity theft,

[2534] Barry M. Leiner et al., "A Brief History of the Internet," ACM SIGCOMM Computer Communication Review, Vol. 39, No. 5 (2009), 22.

cyberterrorism, privacy invasion, and increasingly, sexual offences in the digital domain. Among these, digital sexual abuse represents a complex and rapidly evolving category of harm that challenges traditional legal frameworks premised upon physical proximity and corporeal violation.

Digital sexual abuse includes conduct such as non-consensual dissemination of intimate images, deepfake pornography, sextortion, cyberstalking, online sexual harassment, morphing, doxxing with sexual threats, and child sexual exploitation material (CSEM). These acts undermine sexual autonomy, dignity, privacy, and psychological integrity, often producing harm equal to or exceeding that of offline sexual offences.

## III. CONCEPT OF DIGITAL SEXUAL ABUSE

### 3.1. International Perspective

For decades, international law lacked a comprehensive treaty specifically addressing cybercrime. The first significant international instrument was the Convention on Cybercrime (2001), adopted under the auspices of the Council of Europe.[2535] The Convention harmonizes substantive criminal law provisions relating to illegal access, data interference, system interference, computer-related fraud, and content-related offences such as child pornography. It also establishes procedural powers for search and seizure of computer data and mandates safeguards for human rights and the rule of law.

More recently, the United Nations Convention Against Cybercrime was adopted by the UN General Assembly in December 2024.[2536] This Convention aims to establish a global framework for combating cybercrime, enhancing international cooperation, and standardizing the collection and exchange of electronic evidence. It includes provisions criminalizing child sexual abuse material, fraud, and unauthorized access while emphasizing human rights compliance. Although many States have enacted domestic cybercrime legislation, the emergence of digital sexual abuse underscores the continuing necessity for harmonized global standards.

The World Health Organization (WHO) defines sexual abuse as actual or threatened physical intrusion under coercive circumstances. Sexual exploitation is defined as the abuse of vulnerability or differential power for sexual purposes. Together, these are termed Sexual Exploitation and Abuse (SEA), encompassing all sexual activity with persons under 18 years.[2537]

The United Nations High Commissioner for Refugees (UNHCR) expands this understanding to include sexual harassment, defined as unwelcome sexual conduct likely to cause humiliation or offence.[2538] Importantly, contemporary interpretations extend these definitions beyond workplace contexts into digital environments. WHO further defines sexual violence as any sexual act or attempt obtained through coercion, including non-physical acts.[2539] This broader framing allows inclusion of non-consensual image sharing and online sexual exploitation within the ambit of sexual violence.

Similarly, the UN Special Rapporteur on Violence Against Women has clarified that sexual violence includes acts that violate sexual autonomy even in the absence of physical contact. This normative shift is central to recognizing digital sexual abuse as a legitimate form of sexual violence.

The right to privacy forms a foundational basis for recognizing digital sexual abuse as a human rights violation. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary interference with privacy, honour, and reputation.[2540] The UN Human Rights Committee has interpreted this provision

[2535] Convention on Cybercrime, 2001 (Budapest Convention).
[2536] United Nations Convention Against Cybercrime, adopted by UNGA, 24 December 2024.
[2537] World Health Organization, Sexual Exploitation and Abuse: Definitions (WHO Guidelines).
[2538] UNHCR, Policy on Protection from Sexual Exploitation and Abuse (2003).
[2539] World Health Organization, World Report on Violence and Health (2002).
[2540] International Covenant on Civil and Political Rights, 1966, Art. 17.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

to include protection of personal data in digital contexts. Similarly, the Universal Declaration of Human Rights (UDHR) declares in Article 1 that all human beings are born free and equal in dignity and rights.[2541] Digital sexual abuse directly undermines dignity through humiliation, objectification, and loss of control over one's sexual identity.

Gender-based violence has been recognized under the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). The CEDAW Committee acknowledges that gender-based violence increasingly manifests in digital environments through online harassment, cyberstalking, and unauthorized image sharing.[2542] Protection of children is strengthened under the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC), which mandates criminalization of child pornography across mediums.[2543]

International law, therefore, does not provide a single definition of digital sexual abuse; rather, the concept emerges from the convergence of norms relating to sexual violence, exploitation, privacy, dignity, and gender equality.

### 3.2. Indian Perspective

India, as the world's second-largest internet market, witnessed over 560 million users by 2019.[2544] The digital expansion has corresponded with a surge in technology-facilitated sexual offences, particularly during the COVID-19 pandemic. Indian law addresses digital sexual abuse through a fragmented statutory structure:

- Information Technology Act, 2000[2545] (IT Act)
- Bharatiya Nyaya Sanhita, 2023[2546] (BNS)
- Protection of Children from Sexual Offences Act, 2012[2547] (POCSO)
- Digital Personal Data Protection Act, 2023[2548] (DPDPA)

The IT Act criminalizes publication and transmission of obscene and sexually explicit content (Sections 67, 67A, 67B).[2549] The BNS incorporates offences such as sexual harassment, voyeurism, and stalking (Sections 75, 77, 78,).[2550] POCSO explicitly criminalizes child pornography and online sexual exploitation. However, none of these statutes provide a consolidated definition of digital sexual abuse nor do they adequately address AI-generated sexual content or deepfakes. The Supreme Court's recognition of informational privacy as a fundamental right in ***Justice K.S. Puttaswamy v. Union of India***[2551] strengthens constitutional protection against digital sexual violations which can be inferred to be an intrinsic part of right to privacy.

**FORMS OF DIGITAL SEXUAL ABUSE**

1. **Non-Consensual Intimate Image Sharing (Revenge Porn):** Non-consensual pornography involves dissemination of intimate images without consent. Article 16 of the UN Convention Against Cybercrime criminalizes intentional dissemination of intimate images without authorization. In India, the landmark conviction in the ***State of West Bengal v. Animesh Boxi***[2552] marked the first reported case of non-consensual pornography. The accused was convicted under IPC and IT Act provisions for uploading intimate content of his former partner. Despite such convictions, NCRB data (2022) records 6,896 cases related to transmission of sexually explicit content, indicating systemic underreporting and

[2541] Universal Declaration of Human Rights, 1948, Art. 1.
[2542] CEDAW Committee, General Recommendation No. 35 (2017).
[2543] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2000.
[2544] Telecom Regulatory Authority of India (TRAI), Annual Report 2019.
[2545] Information Technology Act, 2000 (No. 21 of 2000).
[2546] Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023).
[2547] Protection of Children from Sexual Offences Act, 2012 (No. 32 of 2012).
[2548] Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
[2549] Information Technology Act, 2000 (No. 21 of 2000): ss. 67, 67A, 67B.
[2550] Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023): ss. 75, 77, 78.
[2551] (2017) 10 SCC 1.
[2552] 2019 SCC OnLine Cal 384.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

absence of specific offence categorization for adult image-based abuse.[2553]

2. **Deepfake Pornography:** Deepfake pornography refers to AI-generated sexual content superimposing a person's likeness onto explicit material without consent. It relies on machine learning models such as Generative Adversarial Networks (GANs). India currently lacks a specific statutory provision criminalizing deepfake pornography. Although policy discussions on AI regulation are underway, legislative clarity remains absent. Deepfake abuse undermines consent, distorts identity, facilitates extortion, and causes irreversible reputational harm. Its synthetic nature complicates detection and evidentiary processes.[2554]
3. **Sextortion:** Sextortion involves coercing victims by threatening to release intimate content unless demands for money or sexual acts are met. It frequently occurs through fake profiles on social networking sites, dating apps, and messaging platforms.[2555] While extortion and obscenity laws may apply, sextortion lacks a specific statutory definition in Indian law.
4. **Sexual Harassment and Cyberstalking:** Sexual harassment is statutorily defined under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (POSH Act). Its constitutional foundation lies in ***Vishaka v. State of Rajasthan*** where the Supreme Court held that sexual harassment violates Articles 14, 19(1)(g), and 21 of the Constitution.[14] Cyberstalking is recognized under Section 78 of the BNS. It includes persistent monitoring, unsolicited contact, and digital surveillance causing fear or distress.
5. **Child Sexual Exploitation Material (CSEM):** CSEM includes depiction of minors engaged in sexual activity. POCSO and IT Act provisions criminalize creation, possession, and distribution. Emerging forms include livestreamed abuse and AI-generated child sexual content. The OPSC and UN Convention on the Rights of the Child mandate robust criminalization and international cooperation.[2556]
6. **Doxxing with Sexual Threats:** Doxxing involves unauthorized dissemination of personal data to facilitate harassment. When accompanied by sexual threats, it becomes a form of technology-facilitated gender-based violence.[2557] While not explicitly criminalized, such acts may fall under privacy violations and cyber harassment statutes.
7. **Morphing and Identity Theft:** Morphing refers to unauthorized manipulation of images into sexually explicit forms. Though not expressly defined in Indian law, it may be prosecuted under IT Act Sections 67 and 67A.[2558] Identity theft, punishable under Section 66C of the IT Act, often facilitates digital sexual abuse through impersonation and fake profiles.[2559]

## ROLE OF TECHNOLOGY IN FACILITATING DIGITAL SEXUAL ABUSE

1. **End-to-End Encryption:** End-to-end encryption (E2EE) ensures that only communicating users can access

[2553] National Crime Records Bureau, Crime In India, Statistics, Volume II (2022).
[2554] Furizal *et al,* "Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review Author links open overlay panel." *available at:* https://www.sciencedirect.com/science/article/pii/S2590291125006102
[2555] Dr. Murangira B. Thierry, "Cyber Sextortion: An Emerging Threat to Netizens" 14 Health Informatics Journal 2 (2025).
[2556] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornographyUN Convention on the Rights of the Child, *available at:* https://docs.un.org/en/CRC/C/OPSC/LIE/1
[2557] Tufts University, University Police, "Doxxing and Social Media - How to Protect Yourself Against Doxxing", *available at:* https://police.tufts.edu/safety/doxxing-and-social-media
[2558] Information Technology Act, 2000 (No. 21 of 2000): ss. 67, 67A.
[2559] Information Technology Act, 2000 (No. 21 of 2000): s. 66C.

message content. While safeguarding privacy, it obstructs investigation of CSEM and non-consensual image circulation. Tension arises between Article 21 privacy rights and the State's duty to prevent exploitation.[2560]

2. **VPNs and Anonymity:** Virtual Private Networks mask IP addresses, complicating offender identification.[2561] The IT Act's extraterritorial jurisdiction (Section 75) remains difficult to enforce in practice.[2562]
3. **Cloud Servers and Jurisdictional Challenges:** Cloud storage enables indefinite preservation and redistribution of abusive material. Cross-border hosting requires reliance on Mutual Legal Assistance Treaties (MLATs), often delaying victim relief.[2563]
4. **Artificial Intelligence and Synthetic Media:** AI-driven generative technologies have drastically lowered barriers to creating sexualized content.[2564] The absence of AI-specific offences in Indian law results in interpretative inconsistencies and under-criminalization.

## NEED FOR CHANGES IN INDIA'S LEGISLATIVE FRAMEWORK

The exponential growth of digital technologies has fundamentally transformed the nature of sexual harm. While Indian criminal jurisprudence traditionally conceptualized sexual offences as corporeal violations requiring physical proximity, digital sexual abuse operates through technological mediation, anonymity, and borderless dissemination. The existing legislative framework comprising the Information Technology Act, 2000[2565] (IT Act), the Bharatiya Nyaya Sanhita, 2023[2566] (BNS), the Protection of Children from Sexual Offences Act, 2012[2567] (POCSO), and the Digital Personal Data Protection Act, 2023[2568] (DPDPA) addresses fragments of this phenomenon but lacks doctrinal coherence and technological foresight. Consequently, a comprehensive legislative overhaul is imperative.

### Absence of a Statutory Definition of Digital Sexual Abuse

A primary lacuna in Indian law is the absence of a consolidated statutory definition of "digital sexual abuse." The IT Act criminalizes publication and transmission of obscene and sexually explicit material under Sections 67, 67A and 67B, yet these provisions are content-centric rather than consent-centric. They do not explicitly recognize non-consensual dissemination of intimate images of adults as a distinct violation of sexual autonomy.[2569]

The Supreme Court's recognition of privacy as a fundamental right under Article 21 in ***Justice K.S. Puttaswamy v. Union of India***[2570] establishes informational self-determination as constitutionally protected.[2571] Non-consensual image sharing, deepfake pornography, and sextortion directly infringe decisional and informational privacy. However, the absence of a specific offence grounded in violation of sexual autonomy results in reliance on general obscenity or defamation provisions, which inadequately capture the gendered and dignity-based harm involved. A dedicated statutory definition should recognize digital sexual abuse as any technology-facilitated act that violates sexual autonomy, dignity, privacy, or bodily integrity, irrespective of physical contact.

[2560] IBM, "What is End-to-End Encryption?" *available at:* https://www.ibm.com/think/topics/end-to-end-encryption
[2561] ICT Limited v. Ashok Kumar and Others, I.A. 7995/2020.
[2562] Information Technology Act, 2000 (No. 21 of 2000): s. 75.
[2563] Munirah Maher Alshabibi *et al.*, "Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review" *available at:* https://www.mdpi.com/2073-431X/13/8/213#:~:text=The%20challenges%20in%20cloud%20investigation,complicates%20this%20process%20%5B8%5D.
[2564] Furizal *et al,* "Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review Author links open overlay panel." *available at:* https://www.sciencedirect.com/science/article/pii/S2590291125006102
[2565] Information Technology Act, 2000 (No. 21 of 2000).
[2566] Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023).
[2567] Protection of Children from Sexual Offences Act, 2012 (No. 32 of 2012).
[2568] Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
[2569] Information Technology Act, 2000 (No. 21 of 2000): ss. 67, 67A, 67B.
[2570] (2017) 10 SCC 1.
[2571] Constitution of India (No. 1 of 1950): art. 21.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

**Inadequacy in Addressing AI-Generated Sexual Content**

The rise of deepfake pornography and AI-generated intimate imagery exposes significant gaps in Indian criminal law. Generative AI models enable creation of hyper-realistic explicit content without the victim's participation. Existing provisions under the IT Act or BNS may be invoked indirectly, but none explicitly criminalize synthetic sexual fabrication. The harm caused by deepfakes is not merely reputational; it constitutes identity distortion and sexual objectification. The constitutional guarantee of dignity, flowing from Articles 14 and 21, as interpreted in ***Puttaswamy***[2572], demands legislative recognition of AI-driven violations.[2573]

Furthermore, evidentiary challenges in proving authorship and manipulation necessitate procedural reforms. A reformed framework must:

1. Criminalize creation and distribution of AI-generated sexual content without consent;
2. Introduce presumptions in favour of victims regarding authenticity disputes;
3. Mandate rapid takedown mechanisms with strict timelines;
4. Provide for technological watermarking and traceability safeguards compatible with privacy standards.

**Fragmented Approach to Image-Based Sexual Abuse**

The conviction in ***State of West Bengal v. Animesh Boxi***[2574] marked a judicial acknowledgment of non-consensual pornography as a serious offence. However, the prosecution relied upon IPC and IT Act provisions not specifically tailored to image-based abuse. This piecemeal application results in inconsistent sentencing and limited victim compensation. Unlike POCSO which provides a specialized, child-centric procedural and substantive framework, adult victims lack a comparable statutory regime. The need of the hour is a specialized Digital Sexual Abuse Prevention Act, which consolidates offences such as:

- ➔ Non-consensual intimate image sharing;
- ➔ Sextortion;
- ➔ Morphing and identity-based sexual impersonation;
- ➔ Doxxing accompanied by sexual threats;
- ➔ AI-generated sexual fabrication.

Such legislation must emphasize consent as the cornerstone of sexual autonomy rather than obscenity as the threshold of criminality.

**Strengthening Intermediary Accountability**

Digital sexual abuse proliferates through social media platforms, encrypted messaging services, and cloud storage systems. While the IT Act provides safe harbour protection to intermediaries subject to due diligence, enforcement remains inconsistent. Given the constitutional balancing between privacy and free speech, as articulated in ***Shreya Singhal v. Union of India***[2575], intermediary liability must be carefully structured. Nevertheless, safe harbour cannot operate as a shield against deliberate inaction in cases of sexual exploitation.

Reforms should include:

- ➔ Statutory obligation for expeditious takedown of intimate content upon verified complaint;
- ➔ Grievance redressal officers with mandatory response timelines;
- ➔ Transparency reporting on digital sexual abuse complaints;
- ➔ Algorithmic accountability to prevent amplification of exploitative content.

[2572] (2017) 10 SCC 1.
[2573] Constitution of India (No. 1 of 1950): arts. 14, 21.
[2574] 2019 SCC OnLine Cal 384.
[2575] (2015) 5 SCC 1.

These measures must operate alongside procedural safeguards to prevent misuse and over-censorship.

**Victim-Centric Procedural Reforms**

Digital sexual abuse often results in psychological trauma, social ostracization, and reputational harm. However, existing criminal processes remain adversarial and cumbersome. Inspired by the jurisprudence in ***VISHAKA v. State of Rajasthan***[2576] which recognized sexual harassment as a violation of fundamental rights, legislative reform must foreground dignity and victim protection.

Victim-centric reforms should include:

1. Statutory anonymity protections in all digital sexual abuse proceedings;
2. Specialized cyber forensic units with trained personnel;
3. Time-bound removal orders enforceable across jurisdictions;
4. Compensation funds and mandatory psychological counselling;
5. Extraterritorial enforcement mechanisms strengthened through international cooperation.

Without swift remedial relief, digital content may remain perpetually accessible, perpetuating harm indefinitely.

**Jurisdictional and Investigative Challenges**

The borderless nature of digital platforms renders traditional territorial jurisdiction inadequate. Section 75 of the IT Act provides extraterritorial application[2577] yet enforcement depends upon Mutual Legal Assistance Treaties (MLATs), often resulting in delay. Moreover, end-to-end encryption and VPN technologies complicate attribution. Legislative reform must therefore integrate procedural innovation, including:

- Cross-border evidence-sharing frameworks;
- Technology-neutral drafting to future-proof the statute;
- Judicial oversight mechanisms for traceability requests consistent with proportionality standards under Article 21.[2578]

Balancing privacy and public interest remains crucial. However, as the ***Puttaswamy*** judgment clarifies, privacy is not absolute and may be restricted by law satisfying necessity and proportionality tests.[2579]

**Need for a Comprehensive and Harmonized Framework**

India's current approach reflects statutory fragmentation rather than systemic coherence. International developments such as the Budapest Convention and the UN Convention Against Cybercrime underscore the importance of harmonized definitions and cooperation standards. A comprehensive Indian framework must:

- ➔ Provide a unified statutory definition of digital sexual abuse;
- ➔ Recognize AI-generated sexual harm as a specific offence;
- ➔ Shift focus from obscenity to consent and autonomy;
- ➔ Strengthen intermediary obligations;
- ➔ Institutionalize victim-centric remedies;
- ➔ Enhance investigative capacity and cross-border enforcement.

In the digital age, sexual violence has transcended physical space. Law must evolve correspondingly. Failure to adapt risks normalizing algorithmic exploitation and perpetuating gendered harm. A rights-based, technologically responsive, and gender-sensitive legislative reform is no longer

[2576] (1997) 6 SCC 241.
[2577] Information Technology Act, 2000 (No. 21 of 2000): s. 75.
[2578] Constitution of India (No. 1 of 1950): art. 21.
[2579] (2017) 10 SCC 1.

optionalit is constitutionally mandated to safeguard dignity, autonomy, and privacy in India's digital democracy.

**CONCLUSION**

Digital sexual abuse represents a paradigm shift in understanding sexual harm. No longer confined to physical proximity, sexual violence now manifests through algorithmic manipulation, encrypted messaging, anonymized networks, and transnational platforms. International law provides fragmented normative guidance through conventions on cybercrime, gender equality, child protection, privacy, and dignity. Indian law similarly addresses digital sexual abuse through scattered statutory provisions but lacks a unified, technologically responsive framework.

The rapid rise of generative AI, deepfake pornography, and encrypted digital ecosystems exposes significant legal lacunae. There is an urgent need for:

1. A statutory definition of digital sexual abuse;
2. AI-specific criminal provisions;
3. Strengthened intermediary accountability;
4. Enhanced cyber forensic capacity;
5. Victim-centric remedies including swift takedown mechanisms and anonymity safeguards.

A comprehensive legislative response, akin to the specialized framework of POCSO for children, is imperative to safeguard dignity, autonomy, and privacy in the digital age.