SEXUAL VIOLENCE IN THE DIGITAL AGE: LAW, TECHNOLOGY, AND THE PURSUIT OF JUSTICE

Priyanka Nair, Research Scholar, Hidayatullah National Law University, Raipur[1]

ABSTRACT

The convergence of digital technology and sexual violence has produced a crisis that tests the limits of contemporary law. This paper examines the principal forms of technology-facilitated sexual violence that is non-consensual intimate image sharing, online sexual harassment, cyber-stalking, child sexual abuse material, sextortion, and artificial intelligence-generated sexual imagery and through the lens of Indian and comparative law. It argues that India's existing legislative framework, rooted in the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, is structurally inadequate because it is framed around obscenity rather than consent and autonomy. Drawing on UK, EU, and Australian models, the paper proposes a tripartite reform agenda: standalone consent-based offences, mandatory platform liability, and survivor-centred procedural reform. Throughout, the paper situates its analysis within the constitutional framework of Articles 14, 19, and 21, arguing that dignity, equality, and privacy must be the organising principles of any adequate legal response.

Keywords: Digital sexual violence, NCII, sextortion, deepfakes, IT Act 2000, BNS 2023, POCSO, platform liability, privacy, Article 21.

[1] Priyanka Nair, Research Scholar, Hidayatullah National Law University, Raipur.

I. Introduction

The internet promised emancipation. Digital spaces seemed to provide women, LGBTQ+ people and marginalised communities with a safe haven from the physical monitoring and violence of the outside world, a space for self-building, working and political activity. The promise has been broken and broken in many ways. Sexual violence didn't go away when the digital age came – it changed, expanded and discovered new avenues of harm that the law was completely unready to deal with. Technology-facilitated gender-based violence (TFGBV) is considered by the United Nations Special Rapporteur on Violence against Women and Girls to be one of the most rapidly growing human rights crises of the modern age.[2]

In India, the National Crime Records Bureau documented a steep annual increase in cybercrime against women in its 2022 report, yet scholars and civil society organisations have consistently observed that official statistics dramatically undercount the real prevalence of digital sexual violence, given the stigma attached to victimhood, the procedural barriers to registration of complaints, and the pervasive culture of victim-blaming that deters survivors from engaging with the formal justice system.[3]

Digital sexual violence is an umbrella term encompassing the full range of sexually violent, coercive, and exploitative acts committed through or enabled by digital technologies that produce harms that are emphatically material even when the medium is virtual. Reputational destruction, loss of employment, severance of family and social relationships, severe and prolonged psychological injury, and in the most extreme cases suicide: these are the real-world consequences of acts that law and culture have been prone to dismiss as merely 'online' misconduct. As McGlynn and Rackley have observed, image-based sexual abuse is not a novel category of harm but a contemporary form of a pre-existing pattern of male dominance, control, and the weaponisation of female sexuality.[4] The legal response in India has been fragmented and reactive. The Information Technology Act, 2000 (IT Act), as amended in 2008, and the Indian Penal Code, 1860 (IPC), recently replaced by the Bharatiya Nyaya Sanhita, 2023 (BNS), provide the principal legislative architecture. Neither was designed with digital sexual violence

[2]United Nations Special Rapporteur on Violence Against Women and Girls, 'Technology-Facilitated Gender-Based Violence' (UN Doc A/HRC/50/26, 2022) para 5.
[3]National Crime Records Bureau (NCRB), Crime in India 2022 (Ministry of Home Affairs, 2023) Chapter 9 (Cyber Crimes against Women).
[4]Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37(3) Oxford Journal of Legal Studies 534, 536.

in mind. The result is a patchwork of provisions, inadequate individually, incoherent collectively, that systematically fails survivors at every stage of the justice process. This paper diagnoses those failures and proposes a structural reform agenda. Part II establishes the conceptual framework of digital sexual violence and the gendered power relations it reflects. Part III analyses the major forms of digital sexual violence and their distinctive harms. Part IV critically evaluates the Indian legal framework. Part V offers a comparative analysis of international approaches. Part VI addresses platform accountability. Part VII examines the constitutional dimensions of digital sexual violence law. Part VIII concludes with concrete reform proposals.

II. Conceptual Framework: Violence, Technology, and Gender

A. Reframing 'Digital' Violence

A preliminary conceptual move is necessary: the qualification 'digital' must not be permitted to diminish the legal or moral seriousness of the harms under consideration. The term 'online' harm carries a persistent connotation of unreality — as though the virtual character of the medium renders the violence less authentic, the suffering less acute, the legal wrong less serious. This framing is empirically false and normatively dangerous. Contemporary social, professional, and civic life is constituted to a substantial degree through digital platforms; harm to one's digital identity and presence is harm to one's real-world interests. The Cyber Civil Rights Initiative has documented that 93% of non-consensual intimate image (NCII) victims experience significant emotional distress, with over half reporting suicidal ideation.[5] Digital sexual violence is best understood as the extension into technological space of pre-existing structures of gender-based domination. The perpetrator's purpose is rarely reducible to sexual gratification; it is more fundamentally the assertion of power over the victim, the humiliation, the silencing, the punishment of women and LGBTQ+ individuals who fail to conform to prescribed roles. This insight has profound implications for legal design: a law that frames digital sexual violence as an affront to public decency rather than an assault on individual autonomy will systematically mischaracterise the wrong it purports to address.

[5]Danielle Keats Citron and Mary Anne Franks, 'Criminalizing Revenge Porn' (2014) 49 Wake Forest Law Review 345, 347.

B. The Structural Features of Digital Environments

Several structural characteristics of digital environments shape both the modalities and the magnitude of digital sexual violence. Scale and permanence: a single intimate image uploaded to the internet can be replicated, cached, and distributed across millions of devices within hours, and can persist indefinitely on servers distributed across multiple jurisdictions, defying any individual removal effort. Anonymity: perpetrators can operate behind pseudonyms, encrypted networks, and disposable accounts, frustrating identification and prosecution. Platform architecture: social media platforms and content-hosting services have been designed to optimise engagement and virality, not user safety; their algorithmic amplification of controversial and emotionally provocative content systematically facilitates the spread of intimate imagery and harassment campaigns. Transnationality: perpetrators and victims may be located in different countries, or content may be hosted in a third jurisdiction, creating acute enforcement challenges for national legal systems. These features collectively explain why digital sexual violence is not merely equivalent to its offline analogues but constitutes a qualitatively distinct and in many respects more severe form of harm.

III. Manifestations of Digital Sexual Violence

A. Non-Consensual Intimate Image Sharing

Non-consensual intimate image sharing (NCII) is the distribution of sexually explicit images or recordings of a person without their consent, whether images originally shared consensually in an intimate relationship or obtained through hacking, malware, or covert recording, is among the most prevalent and psychologically devastating forms of digital sexual violence. The widely used term 'revenge pornography' is both descriptively misleading and normatively harmful: it implies a proportionate retaliatory character, and its framing around 'pornography' invokes obscenity rather than autonomy as the relevant legal concept. Citron and Franks, in their foundational analysis of NCII law, argued that the correct framework is non-consensual distribution of intimate imagery as a privacy and dignity violation.

In India, NCII is addressed by Section 66E of the IT Act (capturing and publishing images of private areas without consent, punishable by up to three years' imprisonment or a fine of Rs 2 lakh)[6] and Section 67A (publishing or transmitting sexually explicit material electronically,

[6]Information Technology Act 2000 (Act 21 of 2000), s 66E: punishment up to three years' imprisonment or fine of Rs 2 lakh.

punishable by up to five years on first conviction).[7] Neither provision is adequate: Section 66E is narrowly drafted to cover 'private areas' of the body and does not capture full-body intimate images or non-visual sexual recordings; Section 67A is framed around obscenity, requiring a community standards assessment that wholly displaces the consent-based nature of the wrong. India lacks a standalone NCII offence, a gap that the Law Commission of India identified in its 2023 Report No. 289 as requiring urgent legislative redress.[8]

B. Online Sexual Harassment and Cyberflashing

Online sexual harassment encompasses a broad and varied set of conduct: the unsolicited sending of explicit images or messages ('cyberflashing'); the targeted deployment of sexualised abuse in public online forums; coordinated 'pile-on' harassment campaigns involving hundreds or thousands of abusive messages directed at a single individual; doxing accompanied by threats of sexual violence; and the creation of fake sexual profiles of victims. The defining characteristic of much online sexual harassment is its capacity for scale and coordination, loosely organised communities of perpetrators acting in concert through platforms and forums can subject a single target to a volume of abuse utterly without parallel in offline harassment.[9]

Amnesty International's 2018 report on abuse against women on Twitter documented the systematic exposure of women politicians, journalists, and activists to sexualised abuse, finding that members of multiply-marginalised groups, women of colour, LGBTQ+ women, women with disabilities — faced intersectional forms of violence that combined misogyny with racism, homophobia, and caste-based abuse. The psychological and practical consequences include withdrawal from online participation (with consequent damage to professional and civic engagement), self-censorship, depression, anxiety, and, for public figures, a demonstrable chilling effect on free expression that constitutes a structural assault on democratic discourse.

C. Technology-Facilitated Stalking

Digital technologies have dramatically extended the reach and intensity of stalking and intimate partner surveillance. 'Stalkerware' is a commercially available software designed to covertly

[7]Information Technology Act 2000, s 67A: punishment on first conviction up to five years and fine; subsequent conviction up to seven years and fine.
[8]Law Commission of India, Report No. 289, 'Image-Based Sexual Abuse' (2023) para 4.2.
[9]Amnesty International, 'Toxic Twitter: Violence and Abuse Against Women Online' (Amnesty International, 2018) 6.

monitor a target's location, communications, calls, and activities is a tool of pervasive surveillance deployed overwhelmingly in intimate partner violence contexts. Smart home devices, GPS location-sharing features, cloud account access, and keyloggers are also weaponised for continuous monitoring. The result is a form of total surveillance that is invisible to the victim and extremely difficult to escape. Stalking is criminalised under Section 354D IPC and its successor Section 78 BNS, but neither provision specifically addresses stalkerware as a distinct instrument of harm.[10]

D. Child Sexual Abuse Material and Online Grooming

Child sexual abuse material (CSAM) — terminology now preferred over the euphemistic 'child pornography' — represents the most severe form of digital sexual violence, involving the direct exploitation and abuse of children both in its production and in its distribution and consumption. The Supreme Court's judgment in Attorney General for India v. Satish (2021) clarified that no skin-to-skin physical contact is required for conduct to constitute sexual assault under POCSO,[11] a ruling with important implications for online conduct that facilitates or constitutes abuse of children. Sections 13-15 of the POCSO Act[12] and Section 67B of the IT Act[13] provide a relatively comprehensive criminal framework for CSAM, though online grooming, the preparatory process by which adults cultivate trust with children online lacks a specific standalone offence.

E. Sextortion and Deepfake Sexual Imagery

Sextortion is the use of real or fabricated intimate images as leverage to extort money, additional sexual imagery, or sexual acts that has emerged as one of the fastest-growing categories of cybercrime. It may be perpetrated by intimate partners or former partners as an instrument of coercive control, or by transnational criminal networks operating at industrial scale, targeting victims identified through social media and dating applications. India lacks a specific sextortion offence; prosecutions proceed unsatisfactorily under combinations of

[10]Indian Penal Code 1860, s 354C (voyeurism); Bharatiya Nyaya Sanhita 2023, s 77 (successor provision).
[11]Attorney General for India v. Satish & Anr (2021) INSC 762 (Supreme Court of India), overruling State of Maharashtra v. Libnus (2021) Bom HC.
[12]Protection of Children from Sexual Offences Act 2012 (Act 32 of 2012), ss 13-15 (use of child for pornographic purposes).
[13]Information Technology Act 2000, s 67B: punishment on first conviction up to five years; subsequent conviction up to seven years.

IPC/BNS provisions on extortion and the IT Act's electronic content provisions.[14]

Deepfake sexual imagery is the creation, using generative artificial intelligence, of photorealistic sexual images or videos featuring a real person without their consent and represents the most technologically novel and potentially the most far-reaching form of digital sexual violence. The critical distinction from NCII is that the depicted event need never have occurred: any person with access to publicly available images of another person's photographs from social media, professional websites, or press archives can manufacture convincing sexual imagery of that person. The harms are identical to those caused by NCII. Neither the IT Act nor the BNS 2023 contains a provision specifically addressing AI-generated non-consensual sexual imagery, a legislative gap of serious dimensions.[15]

IV. The Indian Legal Framework: A Critical Assessment

A. The IT Act 2000: Architecture and Deficiencies

The Information Technology Act, 2000, as amended in 2008, is India's primary statutory instrument for digital offences. Its provisions relevant to digital sexual violence — Sections 66E, 67, 67A, and 67B — share a common deficiency: they are organised around the concept of obscenity, a nineteenth-century moral construct, rather than consent and autonomy, the principles required to address the harms of digital sexual violence. Section 66E's narrow focus on 'private areas' of the body leaves full-body intimate images and sexual recordings outside its coverage; Section 67A's obscenity framing requires a community standards assessment wholly irrelevant to whether the victim consented to distribution. The absence of a viewer/possession offence for adult NCII (as distinct from CSAM under Section 67B) represents a further gap, permitting consumption without criminal accountability.

The IT Act's penalty structure also reflects inadequate appreciation of the gravity of NCII and related offences. The maximum three-year sentence for Section 66E and five-year sentence for Section 67A compare unfavourably with the seven-year maximum for Section 67B (CSAM) and with penalties in comparative jurisdictions, sending an implicit normative signal that digital

[14]Mary Anne Franks, 'Drafting an Effective Revenge Porn Law: A Guide for Legislators' (Cyber Civil Rights Initiative, 2015) 3.
[15]Bharat Huria, 'Deepfakes and the Law: Gaps in the Indian Legislative Framework' (2023) 15 Indian Journal of Law and Technology 1, 14.

sexual violence against adults is a lesser wrong. The framework was designed for content regulation in the early internet era; applied to digital sexual violence, it is a category error.

B. The BNS 2023: A Missed Opportunity

The Bharatiya Nyaya Sanhita, 2023, which replaced the IPC with effect from 1 July 2024, was an opportunity to systematically address the legislative gaps in India's response to digital sexual violence. That opportunity was substantially missed. The BNS retains successor provisions to Section 354C IPC (voyeurism, now Section 77 BNS) and Section 354D IPC (stalking, now Section 78 BNS) without significant enhancement. No standalone NCII offence, no sextortion provision, and no provision addressing AI-generated sexual imagery were introduced. The Law Commission's Report No. 289 (2023) on image-based sexual abuse had specifically recommended dedicated offences; its recommendations were not incorporated into the final text.

C. POCSO and the Protection of Children

The Protection of Children from Sexual Offences Act, 2012 provides a more comprehensive framework for child protection, including digital sexual exploitation. The Supreme Court's ruling in AG v. Satish confirmed a broad interpretation of the Act's sexual offence provisions, rejecting the Bombay High Court's extraordinary holding that 'skin-to-skin' physical contact was required. Section 67B of the IT Act supplements POCSO with specific digital CSAM offences. However, the absence of a standalone online grooming offence remains a serious lacuna: grooming is the preparatory architecture of online child sexual abuse, and criminalising only the endpoint of that architecture provides incomplete protection.

D. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA), introduces rights over personal data including a right to erasure and consent-based processing requirements[16] that have potential relevance to digital sexual violence. An individual's intimate images constitute sensitive personal data; the DPDPA's requirements could be invoked against platforms hosting such images. However, the DPDPA is a regulatory framework directed at 'data fiduciaries'

[16]Digital Personal Data Protection Act 2023 (Act 22 of 2023), s 4 (ground for processing personal data); s 12(3) (right of erasure).

(organisations processing data), not at individual perpetrators, and its civil enforcement mechanisms are not designed for the urgent, real-time relief that NCII survivors require. Its contribution to addressing digital sexual violence will depend on implementation and on the willingness of courts to interpret its provisions expansively in favour of data subjects.

V. Comparative Perspectives

A. United Kingdom: The Consent-Centred Approach

The United Kingdom's Online Safety Act 2023 represents the most comprehensive statutory framework for digital sexual violence yet enacted in a common law jurisdiction. It creates specific criminal offences for: sharing intimate images without consent; sharing or threatening to share intimate images as an instrument of coercion; sending non-consensual 'cyberflashing' images; and critically for contemporary technology, creating and sharing 'deepfake' intimate images without consent.[17] Each offence is framed around consent and the victim's autonomy, not around community standards of decency. The Act also imposes positive duties on platforms to prevent users encountering illegal content is a significant departure from the reactive 'notice-and-take-down' model that has long dominated platform regulation.

B. European Union: Platform Accountability and the DSA

The European Union's Digital Services Act 2022 (DSA) addresses digital sexual violence through a framework of platform accountability obligations.[18] Very large online platforms are required to conduct and publish risk assessments of systemic risks arising from their services-including gender-based violence facilitated by their platforms and to implement proportionate mitigation measures. The DSA's notice-and-action mechanism mandates expedited processing of reports of illegal content, while its transparency reporting requirements create public accountability for platform enforcement practices. The GDPR's right to erasure has, separately, been invoked by survivors to require the de-indexing of intimate imagery from search engines, a civil remedy that complements the criminal law architecture.

[17]Online Safety Act 2023 (United Kingdom), ss 188-191 (intimate image abuse offences).
[18]Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act), Art 16 (notice-and-action mechanisms) and Art 26 (transparency reporting).

C. Australia: Specialist Regulatory Infrastructure

Australia's Online Safety Act 2021 established the eSafety Commissioner, a specialist regulator with powers to issue removal notices for NCII and other 'cyber abuse material' within 24 hours of notification, backed by significant civil penalties for non-compliance.[19] The Commissioner also administers a 'Basic Online Safety Expectations' framework that establishes minimum standards for platforms operating in Australia. Australia's approach is instructive for India because it combines federal content removal infrastructure addressing the multi-jurisdictional character of digital harms, with state-level criminal offences, a structure well-suited to India's federal constitutional architecture. The eSafety Commissioner's survivor-led design and its accessible, non-adversarial complaint mechanism offer a model for a specialist Indian digital safety regulator.

D. The United States: Section 230 and Its Limits

The United States presents a cautionary example of the limits of platform immunity in addressing digital sexual violence. Section 230 of the Communications Decency Act provides broad immunity to online platforms for third-party content,[20] substantially insulating them from civil liability for hosting NCII and related material. Successive attempts at federal NCII legislation (the SHIELD Act; the EARN IT Act) have stalled in Congress. At the state level, nearly all jurisdictions now have NCII criminal statutes, producing a patchwork of inconsistent laws. The US experience illustrates that without federal platform accountability reform, criminal law provisions directed at perpetrators alone cannot adequately address digital sexual violence.

VI. Platform Accountability: Beyond Safe Harbour

A. The Section 79 Framework and Its Deficiencies

Section 79 of the IT Act provides 'safe harbour' immunity to intermediaries — a category broad enough to encompass social media platforms, messaging services, and content-hosting sites — for third-party content, conditional on compliance with due diligence requirements and

[19]Online Safety Act 2021 (Australia), s 44 (removal notice power of eSafety Commissioner).
[20]Communications Decency Act 1996 (United States), s 230 (protection for private blocking and screening of offensive material).

expeditious removal of unlawful content upon actual knowledge.[21] The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 impose enhanced obligations on significant social media intermediaries, including grievance officers, monthly compliance reports, and controversial traceability requirements for encrypted messaging services.[22]

For digital sexual violence, however, the Section 79 framework is fundamentally inadequate. The 'actual knowledge' standard requires survivors to identify and report content, placing the burden precisely on those who are most harmed by continued exposure to that content. The 72-hour response window for removal of flagged content is far too slow for harms that spread virally within hours. The framework does not require proactive monitoring or upload filtering for known NCII content, a technological capability already deployed for CSAM through PhotoDNA. And the Section 79 immunity creates structural disincentives for platforms to invest in survivor safety infrastructure, since greater proactivity risks constructive notice and the loss of safe harbour protection.

B. Towards a Duty of Care Model

Reform should move beyond the notice-and-take-down paradigm toward a duty of care model analogous to that introduced by the UK Online Safety Act. Under such a model, platforms bear a positive obligation to take reasonable and proportionate steps to prevent their services from being used to perpetrate digital sexual violence is not merely to remove content when notified. This obligation should include: proactive deployment of NCII detection and prevention technology; hash-matching systems that prevent re-upload of known intimate imagery (analogous to the PhotoDNA system used for CSAM); expedited removal mechanisms (within four hours for reported NCII); dedicated survivor support services; and mandatory transparency reporting on enforcement actions. Failure to meet these obligations should attract significant civil penalties, penalties calibrated to the commercial scale of the platforms concerned.

VII. Constitutional Dimensions

A. Article 21: Privacy, Dignity, and the State's Positive Obligation

[21]Information Technology Act 2000, s 79(3)(b): intermediary loses safe harbour upon receiving actual knowledge of unlawful content and failing to expeditiously remove it.
[22]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Rule 4(2) (proactive monitoring obligations for significant social media intermediaries).

The landmark judgment in K.S. Puttaswamy v. Union of India (2017)[23] declared the right to privacy a fundamental right inhering in Article 21. Justice Chandrachud's plurality opinion identified informational privacy as the right to control personal data and intimate representations of oneself and decisional autonomy, freedom from coercion in intimate decisions, as core dimensions of the right. Digital sexual violence is a direct assault on both. Critically, Puttaswamy affirmed that the state bears a positive obligation not merely to refrain from violating privacy but to protect individuals from privacy violations by non-state actors, including digital perpetrators and platforms.[24] This positive obligation provides constitutional support for mandatory platform accountability measures that might otherwise be resisted on grounds of commercial freedom.

The constitutional link between privacy and dignity, traceable to Maneka Gandhi v. Union of India (1978)[25] and its requirement that any procedure limiting Article 21 rights be fair, just, and reasonable, reinforces the obligation to provide a comprehensive legal framework for digital sexual violence. A law that confines itself to obscenity-based provisions while leaving consent-based violations unaddressed cannot satisfy the standard of procedural fairness that the Constitution demands.

B. Article 14 and the Structural Equality Claim

Digital sexual violence is structurally gendered: it is overwhelmingly perpetrated against women, girls, and LGBTQ+ individuals by men. A legal framework that fails to address this structural dimension fails the constitutional guarantee of equality. The Supreme Court's substantive equality jurisprudence, most recently expressed in Navtej Singh Johar v. Union of India (2018),[26] which distinguished 'constitutional morality' from majoritarian social morality and held that the Constitution's equality guarantee requires the affirmation of the dignity of all persons demands that digital sexual violence law be designed with an understanding of its gendered character. Provisions that treat perpetrators and victims as formally equal actors in a neutrally defined transaction miss the structural inequality that gives the conduct its meaning and produces its harm.

[23]K.S. Puttaswamy v. Union of India (2017) 10 SCC 1 (Supreme Court of India), per Chandrachud J at para 249.
[24]Puttaswamy (n 5) per Chandrachud J at para 301: 'The right to privacy postulates a guarantee against the coercive use of force by the state and by non-state actors.'
[25]Maneka Gandhi v. Union of India AIR 1978 SC 597, per Bhagwati J.
[26]Navtej Singh Johar v. Union of India (2018) 10 SCC 1, per Chandrachud J at para 119.

C. Article 19 and the Proportionality Framework

Criminal provisions targeting digital sexual violence operate as restrictions on Article 19(1)(a) (freedom of speech and expression). The Supreme Court's decision in Shreya Singhal v. Union of India (2015),[27] striking down the sweeping vagueness of Section 66A IT Act established that speech restrictions must satisfy a strict proportionality analysis: they must be for an enumerated permissible purpose, rationally connected to that purpose, minimally impairing of the right, and proportionate in effect. Targeted NCII criminalisation, sextortion offences, and deepfake prohibitions readily satisfy this test: they pursue the compelling objectives of protecting dignity, privacy, and equality; they are narrowly drafted to cover only non-consensual conduct; and their restriction on expression is precisely calibrated to the harm they address.

D. Children's Rights and India's International Obligations

India's obligations under the United Nations Convention on the Rights of the Child (UNCRC) include a positive duty to protect children from all forms of sexual exploitation and abuse.[28] Read with Article 15(3) of the Constitution (special legislative provision for children) and the rights of children recognised in the Court's jurisprudence, these obligations require an active and comprehensive legislative response to digital child sexual exploitation. The absence of a standalone online grooming offence in Indian law is, on this analysis, not merely a legislative gap but a failure to discharge a constitutional and international legal obligation.

VIII. Reform Proposals and Conclusion

A. Legislative Reforms

The following legislative reforms are proposed as a minimum adequate response to the crisis of digital sexual violence in India:

> *First, a standalone non-consensual intimate image offence, framed around consent rather than obscenity, covering physical, digitally transmitted, and AI-*

[27]Shreya Singhal v. Union of India (2015) 5 SCC 1 (Supreme Court of India), striking down s 66A IT Act; proportionality analysis per Nariman J.
[28]United Nations Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, Art 34 (protection from sexual exploitation).

generated intimate imagery, with separate aggravated offences for commercial distribution and distribution to the victim's workplace, family, or educational institution.

Second, a specific sextortion offence, defined as using intimate imagery (real or fabricated) to coerce a person into providing money, sexual acts, or other benefits, with enhanced sentences for offences targeting minors or committed by organised criminal networks.

Third, explicit criminalisation of AI-generated non-consensual sexual imagery, with no requirement that the depicted event occurred, and with specific provisions addressing deepfake technology.

Fourth, a standalone online grooming offence — the preparatory solicitation of children online for sexual purposes — not dependent on the occurrence of physical contact or the completion of further offences.

Fifth, a statutory civil cause of action for NCII and related digital sexual violence, enabling survivors to obtain injunctions, damages, and content removal orders without dependence on the criminal justice system.

B. Platform Accountability Reforms

Platform accountability reforms should include: mandatory proactive NCII detection and hash-matching systems; a statutory 4-hour removal obligation for reported NCII; prohibition on re-upload of known intimate imagery; mandatory survivor support services and dedicated reporting mechanisms; and civil penalties for systemic non-compliance calibrated to platform revenue. A specialist Digital Safety Commissioner, modelled on Australia's eSafety Commissioner, should be established with powers to audit platform compliance, issue binding removal notices, and investigate systemic violations.

C. Procedural and Institutional Reforms

Substantive law reform without procedural reform will fail survivors. Essential procedural reforms include: mandatory identity anonymisation for complainants in digital sexual violence proceedings; prohibition on cross-examination regarding complainant's prior sexual history or

character; specialised training for police, prosecutors, and judiciary in digital evidence handling and trauma-informed approaches; and fast-track proceedings in dedicated courts or divisions. Inter-agency cooperation frameworks for cross-border CSAM and sextortion investigations, including mutual legal assistance treaty mechanisms, are equally essential.

D. Conclusion

Sexual violence in the digital age is not merely a technological problem amenable to technological solutions. It is an expression, in new media, of enduring structures of patriarchal domination that require a fundamentally reconceived legal response. The shift this paper has argued for from obscenity to consent, from reactive notice-and-take-down to proactive platform duty of care, from procedurally indifferent criminal law to survivor-centred justice is not a technical adjustment. It is a jurisprudential revolution, one that must place the constitutional values of dignity, equality, privacy, and autonomy at the centre of every legislative choice. India possesses the constitutional foundations for this revolution. The right to life with dignity under Article 21, the substantive equality guarantee of Article 14, the protection of children under Article 15(3), and the international obligations assumed under the UNCRC together provide a powerful mandate for comprehensive reform. What has been lacking is the legislative will to act on that mandate with the urgency the crisis demands. The survivors of digital sexual violence have waited long enough.