
CYBERCRIME AGAINST WOMEN IN INDIA: LEGAL FRAMEWORK AND CHALLENGES

Aanchal Kumar, BBA LLB, Department of Law, Bharati Vidyapeeth Deemed University,
Paschim Vihar, New Delhi, India

ABSTRACT

The rapid proliferation of internet access, smartphone penetration, and social media usage in India has been accompanied by an alarming rise in technology-facilitated violence against women. Cybercrime against women encompassing cyberstalking, online sexual harassment, voyeurism, morphing, revenge pornography, sextortion, and the non-consensual dissemination of intimate imagery constitutes a distinct and rapidly evolving category of gender-based violence that early penal frameworks were never designed to address. India's legal response has developed through a patchwork of statutes, principally the Information Technology Act, 2000, the Indian Penal Code, 1860 (now substituted by the Bharatiya Nyaya Sanhita,

2023), the Protection of Children from Sexual Offences Act, 2012, and the Digital Personal Data Protection Act, 2023. This article critically examines the statutory architecture governing cybercrime against women in India, traces its judicial interpretation through landmark pronouncements, and evaluates the structural, procedural, and societal barriers that continue to undermine effective enforcement, including underreporting, jurisdictional ambiguity, digital evidence volatility, cross-border data access, and inadequate victim-support infrastructure. Drawing on comparative perspectives from the United Kingdom, the United States, the European Union, and Australia, the article situates India's regulatory response within a global context and proposes targeted reforms including narrower statutory definitions for deepfake enabled abuse, victim-centric procedural safeguards, specialized women-staffed cyber cells, and enhanced platform accountability to strengthen India's response to this expanding threat.

Keywords: Cybercrime Against Women, Information Technology Act 2000, Bharatiya Nyaya Sanhita, Cyberstalking, Online Sexual Harassment, Non-Consensual Intimate Imagery, Digital Privacy, Gender-Based Violence, Cyber Law Reform.

INTRODUCTION

The architecture of any nation's response to crime is inevitably shaped by the technologies through which harm is inflicted. In India, the exponential growth of internet subscribers, the near-universal penetration of smartphones, and the migration of social, professional, and commercial life onto digital platforms have transformed both the scale and the character of violence directed at women. Conduct that once required physical proximity—stalking, intimidation, defamation, voyeurism, and sexual harassment—can now be perpetrated instantaneously, anonymously, and across jurisdictional boundaries through a smartphone screen. Cybercrime against women is not merely an extension of offline gender-based violence into a new medium; it possesses distinct characteristics of virality, permanence, anonymity, and cross-border reach that traditional criminal law categories struggle to capture.

India's statutory response to this phenomenon has been incremental rather than comprehensive. The Information Technology Act, 2000, India's foundational cyber legislation, was drafted primarily to facilitate electronic commerce and digital signatures, and contained no provisions specifically addressing gender-based online harm. It was only through the Information Technology (Amendment) Act, 2008—enacted in the aftermath of rising cybercrime and the 26/11 Mumbai attacks—that provisions addressing identity theft, impersonation, and violation of bodily privacy through electronic means were introduced. A more decisive shift occurred through the Criminal Law (Amendment) Act, 2013, passed in the aftermath of the widely publicized Delhi gang-rape case, which for the first time inserted stalking, voyeurism, and sexual harassment as distinct offenses into the Indian Penal Code, explicitly extending their scope to electronic communication. The enactment of the Bharatiya Nyaya Sanhita, 2023, which replaced the IPC with effect from July 1, 2024, has carried these provisions forward while renumbering and, in places, refining them.

Despite this legislative evolution, significant gaps persist. Emerging harms such as deepfake-enabled abuse, algorithmically amplified harassment, and cross-platform doxxing find no explicit statutory recognition, leaving courts to stretch existing provisions on impersonation, obscenity, and extortion to accommodate new fact patterns. Enforcement is further hampered by underreporting driven by social stigma, inadequately trained police personnel, jurisdictional confusion in cases involving foreign-hosted platforms, and the volatility of digital evidence.

This paper undertakes a critical evaluation of the legal and institutional response to cybercrime

against women in India. The research objectives are fourfold: first, to trace the historical and legislative evolution of cyber law as it pertains to gender-based online harm; second, to critically map the current statutory framework across the IT Act, the IPC/BNS, and allied legislation; third, to examine judicial interpretation of these provisions and the constitutional values underpinning them; and fourth, to identify implementation bottlenecks and propose targeted reforms, informed by comparative practice in other common law jurisdictions. The study employs a doctrinal and analytical methodology, drawing upon statutory text, reported judgments, parliamentary and law commission reports, and comparative legislative material.

HISTORICAL EVOLUTION OF THE LEGAL RESPONSE

The Pre-Internet Framework

Prior to the advent of networked computing in India, gender-based offenses such as harassment, stalking, and outraging modesty were governed exclusively by the Indian Penal Code, 1860. Section 354 penalized assault or criminal force intended to outrage a woman's modesty, while Section 509 criminalized words, gestures, or acts intended to insult a woman's modesty. Section 499 provided a general defamation remedy. These provisions, drafted for a physical-world context, presumed direct, contemporaneous contact between offender and victim and offered no mechanism to address conduct mediated through a screen or transmitted across a network.

The Information Technology Act, 2000 and its 2008 Amendment

The IT Act, 2000 was enacted principally to grant legal recognition to electronic records and digital signatures and to facilitate e-governance and e-commerce. In its original form, it contained no provision targeting online harassment or sexual privacy violations. The Information Technology (Amendment) Act, 2008 substantially expanded the Act's penal scope, introducing Section 66C (identity theft), Section 66D (cheating by personation using computer resources), Section 66E (violation of bodily privacy through capturing or publishing images of a private area), Section 67A (publishing sexually explicit material), and Section 67B (child sexual abuse material). The controversial Section 66A, which criminalized sending 'offensive' messages through communication services, was also inserted at this time; it was later struck down in its entirety by the Supreme Court in *Shreya Singhal v. Union of India* (2015) for vagueness and its chilling effect on free speech, illustrating the tension between protecting individuals from online abuse and safeguarding constitutional speech rights.

The Criminal Law (Amendment) Act, 2013

The gang-rape of a young woman in Delhi in December 2012 catalyzed the Justice J.S. Verma Committee's recommendations, several of which were enacted through the Criminal Law (Amendment) Act, 2013. This amendment inserted Section 354A (sexual harassment, including online contact and demands for sexual favours via electronic means), Section 354C (voyeurism, criminalizing capturing or disseminating images of a woman engaged in a private act without consent), and Section 354D (stalking, expressly extending to monitoring a woman's use of the internet, email, or any other form of electronic communication). This amendment represented the first explicit statutory recognition that gender-based offenses could be committed entirely through digital means.

Consolidation under the Bharatiya Nyaya Sanhita, 2023

The BNS, 2023, which replaced the IPC with effect from July 1, 2024, retained the substance of these 2013 reforms while renumbering them: stalking now appears as Section 78, voyeurism as Section 77, and the insulting-modesty provision as Section 79. The BNS did not, at the time of its enactment, introduce any wholly new offense specific to deepfake-generated sexual imagery, artificial-intelligence-enabled impersonation, or algorithmic harassment, leaving these emerging harms to be addressed through a combination of existing impersonation, obscenity, and privacy provisions.

OVERVIEW OF THE CURRENT LEGAL FRAMEWORK

Cybercrime against women in India is today governed by an overlapping matrix of statutes rather than a single, unified code. The Information Technology Act, 2000 (as amended) supplies the technology-specific offenses; the Bharatiya Nyaya Sanhita, 2023 (successor to the IPC) supplies the gender-specific offenses, several of which are drafted broadly enough to capture electronic conduct; the Protection of Children from Sexual Offences Act, 2012 governs offenses against minors; and the Digital Personal Data Protection Act, 2023 introduces consent and breach-notification obligations relevant where personal data or images are unlawfully processed or leaked. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due-diligence, traceability, and grievance-redressal obligations on social media and other intermediaries, creating a regulatory layer aimed at platform accountability rather than individual offenders.

Comparative Statutory Table

Cyber Offense	IT Act, 2000 Provision	IPC (1860) / BNS (2023) Provision	Nature of Protection
Cyberstalking	No dedicated provision; addressed indirectly via Section 66	Section 354D IPC → Section 78 BNS	Criminalizes monitoring, contacting, or following a woman through electronic communication despite disinterest.
Voyeurism / Non-Consensual Intimate Imagery	Section 66E (violation of privacy)	Section 354C IPC → Section 77 BNS	Punishes capturing, publishing, or transmitting images of a woman's private area without consent.
Publishing/Transmitting Obscene or Sexually Explicit Material	Sections 67, 67A	No direct electronicspecific equivalent; Section 292 IPC applied by analogy → Section 294 BNS	Targets online circulation of obscene content, including revenge pornography.
Morphing, Impersonation and Fake Profiles	Section 66C (identity theft), Section 66D (cheating by personation)	Section 419/469 IPC → Sections 319/336 BNS	Addresses creation of fake accounts and digitally altered images, though deepfake-specific language is absent.
Online Sextortion / Blackmail	Sections 66C, 66D read with Section 43	Section 384 IPC (extortion) → Section 308 BNS	Covers coercion through threats to release intimate content unless demands are met.
Insulting the Modesty of a Woman by Words/Gestures Online	Section 67 (obscene electronic content)	Section 509 IPC → Section 79 BNS	Extends the traditional 'modesty' offense to comments, emojis, and gestures transmitted electronically.
Child Sexual Abuse Material	Section 67B	Protection of Children from Sexual Offences (POCSO) Act, 2012, ss. 13–15	Creates a stringent, victim-specific regime for minors, operating alongside the general penal code.

DEEP-DIVE ANALYSIS OF KEY OFFENSE CATEGORIES

Cyberstalking

Section 354D IPC, carried forward as Section 78 BNS, criminalizes following, contacting, or monitoring a woman's use of the internet, email, or any other form of electronic communication despite a clear indication of disinterest, as well as monitoring her internet usage through spyware or tracking applications. The provision's chief strength lies in its explicit textual recognition of digital monitoring as a form of stalking; its chief weakness lies in continued reliance on police and prosecutorial familiarity with digital forensics to establish the requisite pattern of conduct.

Voyeurism and Non-Consensual Intimate Imagery

Section 354C IPC (Section 77 BNS) and Section 66E of the IT Act jointly address the capturing and circulation of a woman's image without consent. In practice, these provisions are most frequently invoked in cases involving so-called 'revenge pornography' the circulation of intimate images by a former partner without consent. A persistent difficulty is the near-instantaneous, cross-platform virality of such content, which frequently outpaces the statutory and procedural mechanisms available for takedown.

Morphing, Impersonation, and the Deepfake Gap

Digitally morphed or artificial-intelligence-generated ('deepfake') sexualized imagery of women has emerged as one of the most consequential gaps in the current framework. Neither the IT Act nor the BNS contains a provision expressly naming synthetic or AI-generated sexual imagery as a distinct offense. Prosecutors instead rely on a combination of Section 66D IT Act (cheating by personation), Section 66E (privacy violation), obscenity provisions, and defamation law an patchwork approach that leaves interpretive uncertainty as to whether imagery that is technically 'fabricated' but depicts a real, identifiable woman falls within provisions drafted around the capture of an actual image.

Online Sextortion

Sextortion coercing a victim through threats to publish intimate content unless monetary or sexual demands are met is prosecuted through a combination of Section 384 IPC (extortion,

now Section 308 BNS) and the identity-theft and impersonation provisions of the IT Act. The cross-border nature of many sextortion operations, frequently originating from outside India, considerably complicates investigation and enforcement.

Online Sexual Harassment and Trolling

Section 509 IPC (Section 79 BNS) has been judicially extended to cover words, gestures, or visible representations transmitted electronically, including sexually suggestive comments, coordinated trolling campaigns, and gendered abuse in online spaces. Because such conduct is frequently perpetrated by anonymous or pseudonymous accounts, and often by multiple actors acting in loose coordination rather than a single identifiable offender, the applicability of traditional individual-liability-based penal provisions is frequently strained.

JUDICIAL AND CONSTITUTIONAL PERSPECTIVES

The judicial response to cybercrime against women in India has developed along two intersecting tracks: the interpretation of specific penal provisions, and the articulation of broader constitutional values particularly privacy and dignity under Article 21 that inform how those provisions ought to be applied.

In *State of Tamil Nadu v. Suhas Katti* (2004), a Chennai metropolitan magistrate's court delivered what is widely regarded as India's first conviction under the IT Act for online harassment of a woman, involving the posting of obscene and defamatory messages about the victim in an internet chat forum. The case is frequently cited as an early demonstration that existing provisions, despite their limitations, could be marshalled to secure a conviction where investigators gathered sufficient digital evidence.

In *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, the Supreme Court struck down Section 66A of the IT Act in its entirety as unconstitutionally vague and overbroad, holding that it imposed an impermissible chilling effect on speech protected under Article 19(1)(a). While the decision is best known as a free-speech landmark, it also removed a provision that despite its infirmities had occasionally been invoked in cases of online harassment, underscoring the difficulty of legislating against abusive speech without infringing protected expression.

In *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, a nine-judge bench of the Supreme Court recognized the right to privacy, including informational and bodily privacy, as

intrinsic to the right to life and personal liberty under Article 21. This pronouncement has since provided the constitutional foundation for judicial reasoning in cases involving non-consensual intimate imagery, reinforcing that the unauthorized capture or circulation of a woman's image implicates a fundamental right and not merely a statutory interest.

High Courts have, in a growing body of unreported and partially reported orders, recognized a qualified 'right to be forgotten' in the context of intimate images and morphed content circulated online, directing intermediaries to remove such material even where no criminal conviction has yet been secured reflecting judicial willingness to grant urgent equitable relief given the practical impossibility of full retrospective containment once content has gone viral.

IMPLEMENTATION CHALLENGES AND SYSTEMIC BOTTLENECKS

The effectiveness of India's cyber-crime framework as it applies to women is constrained by a number of persistent structural and procedural obstacles.

Underreporting and Social Stigma

A substantial proportion of cybercrimes against women are believed to go unreported due to social stigma, fear of victim-blaming, concerns about family reputation, and apprehension that engaging with the criminal justice process will itself expose the victim to further public scrutiny particularly in cases involving intimate imagery.

Investigative Capacity and Training Gaps

Effective investigation of cyber offenses requires specialized skills in digital forensics, open-source intelligence, and platform-specific evidence preservation. Many district-level police stations continue to lack officers trained in these areas, resulting in delayed First Information Reports, improperly preserved digital evidence, and reliance on external forensic laboratories with significant case backlogs.

Jurisdictional and Cross-Border Complications

A significant share of cybercrime against women involves offenders, servers, or platforms located outside India. Securing data from foreign-headquartered intermediaries typically requires resort to Mutual Legal Assistance Treaties, a process that can take months, during

which harmful content frequently continues to circulate.

Evidentiary Volatility and Platform Cooperation

Digital evidence – chat logs, metadata, IP addresses – can be altered, deleted, or rendered inaccessible within short periods. While the IT Rules, 2021 impose data-retention and grievance-redressal obligations on intermediaries, compliance and response times vary considerably across platforms, and enforcement of these obligations against foreign entities remains limited.

Absence of Dedicated Statutory Language for Emerging Harms

As discussed above, the absence of an explicit statutory category for AI-generated or deepfake sexual imagery forces courts and prosecutors to rely on interpretive extension of provisions never drafted with such technology in contemplation, generating legal uncertainty for victims and defendants alike.

COMPARATIVE ANALYSIS

Analytical Dimension	Pre-2013 Legal Position	Post-2013 / BNS Legal Position
Recognition of Cyberstalking	Absent; victims relied on general IPC provisions such as Section 503 (criminal intimidation) or civil remedies.	Explicitly codified under Section 354D IPC (2013) and carried forward as Section 78 BNS, covering electronic monitoring.
Non-Consensual Intimate Imagery	No specific offense; prosecutions attempted under obscenity law (Section 292 IPC) with limited success.	Section 354C IPC / Section 77 BNS and Section 66E IT Act jointly criminalize capture and circulation without consent.
Anonymous and Pseudonymous Harassment	Largely unaddressed; identifying an anonymous offender required protracted police investigation with no statutory deadlines.	Intermediary Guidelines (IT Rules, 2021) impose traceability and grievance-redressal obligations on platforms, aiding identification.
Data Protection Backdrop	No comprehensive data protection statute; victims of data-based harassment had no dedicated civil remedy.	Digital Personal Data Protection Act, 2023 introduces consent-based processing and breach-notification duties relevant to leaked personal data.

COMPARATIVE INTERNATIONAL PERSPECTIVE

India's evolving framework may usefully be situated alongside comparable reforms in other common law jurisdictions confronting the same technological harms.

United Kingdom: The Online Safety Act, 2023 introduced specific offenses addressing cyberflashing and the non-consensual sharing of intimate images, building upon earlier protections under the Protection from Harassment Act, 1997 and the Malicious Communications Act, 1988. The UK's approach places significant emphasis on platform-level duties of care enforced by the communications regulator Ofcom, in addition to individual criminal liability.

United States: Regulation of online harassment and non-consensual intimate imagery in the United States is primarily a matter of state law, with a majority of states having enacted 'revenge pornography' statutes of varying scope. At the federal level, the SHIELD Act (Stopping Harmful Image Exploitation and Limiting Distribution), enacted in 2022, created a federal criminal offense for the non-consensual distribution of intimate images, supplementing the patchwork of state provisions.

European Union: The Digital Services Act, 2022 imposes harmonized due-diligence and risk-mitigation obligations on large online platforms operating within the EU, including obligations to act expeditiously against illegal content such as non-consensual intimate imagery, complemented by the General Data Protection Regulation's consent-based framework for personal data, including images.

Australia: The Online Safety Act, 2021 empowers the eSafety Commissioner, a dedicated regulatory office, to issue rapid removal notices to platforms hosting non-consensual intimate imagery or cyber-abuse material, backed by statutory penalties for non-compliance a model of administrative, rather than purely criminal, enforcement that has drawn increasing international attention as a potential template for other jurisdictions, including India.

KEY FINDINGS AND POLICY RECOMMENDATIONS

This analysis yields several core findings. First, India's legal response to cybercrime against women has evolved reactively, largely in response to specific triggering events, rather than through comprehensive anticipatory design a pattern evident in the post-2008 and post-2013

waves of amendment. Second, the current framework's reliance on interpretive extension of physical-world offense definitions leaves emerging harms, particularly deepfake-enabled abuse, without clear statutory anchoring. Third, enforcement gaps rooted in training, jurisdiction, and platform accountability persist across an otherwise reasonably comprehensive statutory architecture.

Based on these findings, the following reforms are recommended:

1. **Statutory Recognition of Synthetic and AI-Generated Sexual Imagery:** Parliament should introduce an explicit provision criminalizing the creation, possession, and circulation of digitally fabricated or AI-generated sexually explicit imagery depicting an identifiable woman, removing present reliance on impersonation and obscenity provisions not designed for this harm.
2. **Time-Bound Statutory Takedown Mechanism:** A mandatory, short statutory timeline for intermediary takedown of non-consensual intimate imagery, enforced through the existing IT Rules, 2021 grievance redressal architecture, would materially reduce the harm caused by content virality.
3. **Specialized, Women-Staffed Cyber Cells:** Expansion of dedicated cyber-crime cells at the district level, staffed with trained women officers and equipped with basic digital-forensics capacity, would help address underreporting linked to stigma and discomfort in engaging with male officers.
4. **Victim Anonymity and Procedural Safeguards:** Statutory protection of victim identity throughout investigation and trial in cases involving intimate imagery, akin to protections already available in sexual offense trials, would reduce the disincentive to report.
5. **Strengthened Cross-Border Cooperation:** Streamlined bilateral and multilateral arrangements for expedited data requests to foreign-headquartered platforms, potentially modeled on emerging international frameworks for cross-border electronic evidence sharing, would reduce delays in investigation.

CONCLUSION

The evolution of India's legal response to cybercrime against women from the gender-neutral,

ecommerce-oriented IT Act of 2000, through the post-2008 introduction of privacy and impersonation offenses, to the transformative 2013 amendments and their consolidation in the Bharatiya Nyaya Sanhita, 2023 reflects a gradual but incomplete recognition that digital spaces demand the same protective seriousness historically reserved for physical ones. The framework that has emerged is reasonably comprehensive in addressing established harms such as stalking, voyeurism, and online sexual harassment, but remains structurally unprepared for emerging, technologically sophisticated forms of abuse, particularly synthetic media. Ultimately, the adequacy of India's response will be determined not by the text of its statutes alone, but by the state's capacity to invest in trained investigators, responsive platforms, and victimcentric procedures capable of translating statutory protection into lived safety for women online.

REFERENCES

- [1] Information Technology Act, 2000 (Act No. 21 of 2000).
- [2] Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).
- [3] Indian Penal Code, 1860 (Act No. 45 of 1860).
- [4] Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).
- [5] Criminal Law (Amendment) Act, 2013 (Act No. 13 of 2013).
- [6] Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012).
- [7] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- [8] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- [9] Constitution of India, 1950.
- [10] Ministry of Home Affairs. (2013). Report of the Committee on Amendments to Criminal Law (Justice J.S. Verma Committee). Government of India.
- [11] National Crime Records Bureau. (2023). Crime in India: Statistics on Cyber Crimes Against Women. Government of India.
- [12] Law Commission of India. (2018). Report No. 273: Implementation of the United Nations Convention Against Torture. Government of India.
- [13] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- [14] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- [15] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004, Metropolitan Magistrate's Court, Egmore, Chennai.

- [16] Duggal, P. (2022). *Cyber Law: The Indian Perspective* (5th ed.). Saakshar Law Publications.
- [17] Halder, D., & Jaishankar, K. (2021). *Cyber Crimes Against Women in India* (2nd ed.). SAGE Publications.
- [18] Kumar, A. (2024). Digital Violence and the Limits of the IT Act: A Gendered Reading. *Indian Journal of Law and Technology*, 20(1), 55–79.
- [19] Sharma, N. (2023). Deepfakes and the Gap in Indian Criminal Law. *National Law School Journal*, 15(2), 112– 134.
- [20] UK Online Safety Act, 2023.
- [21] SHIELD Act, 2022 (United States).
- [22] Regulation (EU) 2022/2065 (Digital Services Act).
- [23] Online Safety Act, 2021 (Australia).