

DIGITAL SPACES AND WOMEN'S SAFETY: EXAMINING CYBER CRIMES AGAINST WOMEN UNDER INDIAN LAW

NANCY G. RATHOD

Professor,

V. T. Choksi Sarvajanic Law College

ABSTRACT

The rapid adoption of the internet and digital technology in India has created an exceptional environment for women's empowerment. But at the same time, it has brought new types of violence against women, which are collectively referred to as "cybercrimes against women" (CAW). This paper critically examines the efficacy of the Indian legal framework—specifically the Information Technology (IT) Act, 2000, and relevant provisions within the Bharatiya Nyaya Sanhita (BNS), 2023 (which replaced the IPC)—in addressing these crimes, such as cyberstalking, non-consensual sharing of intimate images (NCII), and digital doxxing. The study uses a doctrinal and analytical research approach to identify important legal and institutional gaps, such as the lack of explicit laws for new threats like deepfakes, the lack of gender sensitivity in law enforcement, and difficulties with handling evidence and jurisdictional issues. The paper concludes by offering actionable policy recommendations aimed at strengthening the legal response, enhancing institutional capacity, and promoting a safer digital environment for women, thereby advocating for their continued rights and empowerment in cyberspace.

Keywords: Cybercrime, Women's Safety, Digital Violence, Indian Law, IT Act, Bharatiya Nyaya Sanhita (BNS).

INTRODUCTION

The theme "Empower HER: Advocating Women's Rights and Empowerment" recognises that true empowerment requires safety and freedom, both in the physical world and in the expanding digital space. India is among the world's largest internet user bases, and for many women, the internet is a vital tool for education, economic independence, and social advocacy. However, this digital inclusion comes with a growing threat. According to recent data, cases of cybercrimes against women (CAW) are continuously rising, with perpetrators often exploiting

the anonymity and reach of digital platforms to commit acts of harassment, blackmail, and sexual violence.¹ The most common forms of CAW include:

1. **Cyberstalking:** Monitoring or contacting a woman repeatedly via electronic means despite her clear disinterest.
2. **Non-Consensual Sharing of Intimate Images (NCII) / Revenge Porn:** Sharing private, sexual images or videos without the subject's permission, often for revenge or blackmail.
3. **Digital Doxxing and Blackmail:** Publishing a victim's private contact information or location online to incite targeted harassment. This paper aims to evaluate how effectively Indian law responds to this new wave of gendered digital violence and to identify crucial areas for reform.

LITERATURE REVIEW

Existing literature on CAW in India consistently highlights two major observations: the rapid increase in reported cases and the fragmented nature of the legal response. Scholars generally agree that the IT Act, 2000, though the primary cyber law, suffers from being gender-neutral and therefore fails to capture the unique dimensions of gendered digital violence.² Provisions like Section 66E (Violation of Privacy) and Section 67A (Publishing Sexually Explicit Material) are essential but are often criticised for being broad or having outdated definitions of "obscurity." The introduction of specific amendments to the IPC in 2013 (e.g., Section 354D for Stalking) and their carry-over into the new Bharatiya Nyaya Sanhita (BNS) 2023 are seen as positive steps towards criminalising certain behaviours like cyberstalking.³ However, research indicates persistent challenges in implementation due to low conviction rates, jurisdictional complexity, and a lack of technological expertise within the police force.⁴ Recent studies further emphasise the urgent need to legally recognise and address emerging threats like Deepfake technology, which allows for the creation of hyper-realistic non-consensual pornography, posing a catastrophic threat to a woman's reputation and mental health.

¹ Government of India. (2024). Crime in India Report (2023). National Crime Records Bureau (NCRB).

² Jain, S. (2025). From Code to Conduct: Analysing the Efficacy of IT Act, 2000 Sections for Digital Safety. Indian Journal of Cyber Law.

³ Government of India. (2023). Bharatiya Nyaya Sanhita, 2023. Ministry of Law and Justice.

⁴ National Commission for Women. (2025). Report on Digital Safety and Women: Challenges and Recommendations. New Delhi: NCW.

OBJECTIVES

The research paper is guided by the following objectives:

1. To analytically examine the key statutory provisions under the IT Act, 2000, and the Bharatiya Nyaya Sanhita (BNS), 2023, relevant to protecting women from digital violence.
2. To critically evaluate the effectiveness and limitations of these laws in prosecuting modern and emerging cybercrimes against women, such as deepfakes and NCII.
3. To identify the major institutional and societal challenges that hinder the effective enforcement of cyber laws against women in India, including underreporting and police sensitisation.
4. To propose concrete legal and policy recommendations for strengthening the legal framework to ensure digital safety and genuine empowerment for women.

RESEARCH METHODOLOGY

This study employs a doctrinal research methodology. It relies on the critical analysis of primary and secondary legal sources:

- ❖ Primary Sources: Statutory texts (The Information Technology Act, 2000; The Bharatiya Nyaya Sanhita, 2023), judicial pronouncements (key Supreme Court and High Court judgments related to privacy and cybercrimes), and government reports (National Crime Records Bureau (NCRB) data).
- ❖ Secondary Sources: Academic journals, law review articles, reports from the National Commission for Women (NCW), and reputable news analysis on cyber safety.

RESEARCH PROBLEM/HYPOTHESIS

Research Problem: Despite the existence of multiple legal provisions under Indian law, the legal mechanism remains inadequate and fragmented in effectively preventing, prosecuting, and providing timely redressal for the evolving and uniquely gendered nature of cybercrimes against women.

Hypothesis: The successful advocacy for women's rights in digital spaces requires not only specific amendments to recognise emerging crimes (like deepfakes) but, more urgently, a massive overhaul of the enforcement and institutional ecosystem through specialised training and gender sensitisation.

ANALYSIS AND INTERPRETATION/FINDINGS

The analysis of the current legal framework reveals several critical findings:

1. Foundational Laws vs. Emerging Threats

Indian law addresses core cybercrimes through a combination of general cyber law (IT Act) and targeted criminal provisions (BNS).

- IT Act Sections (66E, 67, 67A) provide a punitive framework for privacy violations and explicit content.
- BNS Sections (e.g., 77, 78, 79) successfully criminalise behaviour that manifests online, such as cyberstalking and voyeurism, ensuring continuity from the older IPC.
- **IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Amended 2025):** Recent amendments explicitly define "synthetically generated information" and impose a due diligence obligation on social media intermediaries (SSMIs) to combat deepfakes:
 - ✚ **Mandatory Labelling:** Intermediaries that provide AI tools must ensure that all generated content is clearly labelled or embedded with a permanent, unique metadata tag.
 - ✚ **Content Removal:** Platforms are required to act expeditiously to remove unlawful content upon receiving a complaint, typically within 36 hours (or 3 hours during elections).
 - ✚ **Grievance Redressal:** A robust Grievance Appellate Committee system has been established to review user complaints that are not resolved by the platforms.

2. The Enforcement and Sensitisation Gap

Statistics and case studies show a significant gap between reported cases and convictions. The primary reasons for this gap are:

- **Technological Lag:** Police units often lack advanced cyber forensic labs and personnel trained in digital chain-of-custody. The Central Government has provided financial assistance for cyber forensic-cum-training laboratories, but gaps remain in implementation.⁵

⁵ Government of India. (2025, March 18). Lok Sabha Unstarred Question No. 2944 on Cybercrime Against Women. Ministry of Home Affairs.

- **Institutional Bias:** Traditional, patriarchal attitudes often translate into victim-blaming at the police station level, discouraging women from reporting crimes out of fear of social judgment or police apathy.

Jurisdictional Hurdles: Since data crosses state and international borders instantly, identifying and prosecuting perpetrators requires coordination that current law enforcement structures struggle to maintain.

3. Socio-Legal Consequence

The ineffective legal response has profound socio-legal consequences:

- **Silencing Effect:** The threat of digital violence is used to silence women, particularly those who are vocal in political, social, or human rights debates. This violates their right to freedom of expression.
- **Psychological Trauma:** Due to the distinctive character of digital humiliation, victims experience intense and continuous psychological pain, highlighting the necessity of laws requiring victims to receive counselling and support.

CONCLUSION

The title “Digital Spaces and Women’s Safety: Examining Cyber Crimes Against Women under Indian Law” underscores the reality that India’s digital leap must be matched by a secure legal shield for its women citizens. The speed and diversity of digital crimes currently surpass the legal foundation for prosecution established by laws like the IT Act and BNS. The government and judiciary must guarantee that digital rights are considered as fundamental rights and supported by prompt, gender-sensitive, and technologically capable institutional support if the conference's "Empower HER" goal is to be achieved.

SUGGESTIONS/RECOMMENDATIONS

Based on the analysis, the following suggestions are offered to strengthen the legal and institutional framework:

1. **Enactment of a Dedicated NCII Law:** Introduce a standalone, non-bailable provision specifically criminalising the non-consensual creation and sharing of intimate images, with mandatory provisions for platform removal and victim protection.

2. **Establishment of Specialised Cybercrime Units:** Mandate the creation of Gender-Sensitive Cyber Cells in all major districts, staffed by specially trained women officers and technical experts to ensure a safe, confidential, and effective reporting process.
3. **Judicial Capacity Building:** Implement mandatory training modules for judicial officers and public prosecutors on the technicalities of cyber forensics, evidence preservation, and the psychological impact of digital violence. Platform Accountability and Transparency: Strengthen the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, to ensure that platforms adhere to a maximum 24-hour turnaround time for removing NCII and other gendered abuse content upon notification.

REFERENCES

1. Jain, S. (2025). From Code to Conduct: Analysing the Efficacy of IT Act, 2000 Sections for Digital Safety. *Indian Journal of Cyber Law*.
2. Government of India. (2023). *Bharatiya Nyaya Sanhita, 2023*. Ministry of Law and Justice.
3. Government of India. (2024). *Crime in India Report (2023)*. National Crime Records Bureau (NCRB).
4. Ministry of Communications and Information Technology. (2000). *The Information Technology Act, 2000*. New Delhi: The Gazette of India.
5. National Commission for Women. (2025). *Report on Digital Safety and Women: Challenges and Recommendations*. New Delhi: NCW.