TECHNOLOGICAL DISADVANTAGES AGAINST WOMEN: EVALUATING INDIA'S LEGAL AND JUDICIAL FRAMEWORK

Dhruv Jayeshbhai Shah, Faculty of Law, The Maharaja Sayajirao University of Baroda

ABSTRACT

The article examines how digital technologies in India simultaneously expand opportunities for women and intensify gendered vulnerabilities. It first traces the rise of technology facilitated violence against women, including cyberstalking, image-based abuse, deepfakes and financial scams, situating these harms within the digital gender divide and low levels of women's digital literacy. It then analyses the constitutional foundations, statutory provisions under the Information Technology Act 2000 and Bharatiya Nyaya Sanhita 2023, and key judicial decisions such as Suhas Katti and Shreya Singhal to evaluate how far the existing legal and judicial framework responds to these harms. The discussion highlights persistent implementation gaps relating to underreporting, police capacity, platform governance and socio-cultural stigma, arguing that these convert formal safeguards into largely illusory protections. The article concludes by proposing doctrinal, institutional and platform level reforms aimed at realigning "Digital India" with constitutional commitments to equality, dignity and gender-just digital citizenship.

Technology's Dual Effect: Empowerment or Harm for Women?

The development of technology is often hailed as a means of empowering women by giving them access to previously unattainable worldwide networks, financial services, jobs, and education.[1] Digital platforms have made it possible to assert autonomy in both personal and professional spheres and to engage in public discourse.[2] However, women's actual use of digital spaces in India reveals a far more nuanced reality, where discrimination, structural exclusion, and harm enabled by technology coexist with the promise of empowerment.[3]

Many women still have low levels of digital literacy, little control over their devices, and restricted access to secure online environments despite increased connectivity.[4] Women are disproportionately exposed to risks like online harassment, cyberstalking, non-consensual image circulation, identity theft, and financial fraud through digital platforms as a result of the intersection of these limitations with deeply ingrained gender norms and socioeconomic vulnerabilities.[5] As a result, the very instruments intended to promote participation may also be used for abuse, coercion, and surveillance, especially in situations where reporting procedures and safety features are not sufficiently understood.

Lack of knowledge about data protection, privacy protections, and the legal remedies available under India's legislative and regulatory framework causes the problem.[6] Women's ability to seek real protection is further weakened by implementation gaps and ineffectual remedy.[7] This chapter therefore frames the central inquiry of the article: whether the existing legal and judicial framework in India sufficiently addresses the gendered disadvantages produced by technology, or whether it remains inadequate to secure women's rights in digital spaces.

The Dark Side of Technology: Online Abuse and Exploitation of Women

The term "technology-facilitated violence against women" (TFVAW) describes any act of gender-based violence that is carried out, aided, intensified, or amplified using digital

[1]UN Women, *Model Framework for Legislation on Technology-Facilitated Violence Against Women and Girls* 8–10 (2025).
[2] International Center for Research on Women, *Technology-Facilitated Gender-Based Violence in India: Key Trends and Responses* 12 (2021).
[3] IT for Change, *Technology-Mediated Violence Against Women in India: A Review* 5–7 (2017).
[4] National Crime Records Bureau, *Crime in India 2022*, vol. 2, at 156 (2023).
[5] Equality Now, *Experiencing Technology-Facilitated Gender-Based Violence in India* 23–25 (2025).
[6] Samridhi Goyal, Cyber Crimes against Women and Prevention, 10–12 (Chanakya Nat'l L. Univ. 2025).
[7]LawGratis, Challenges to Indian Law and Cyber Crime Scenario in India (July 17, 2025).

technologies.[8] This includes cybercrimes such as harassment, stalking, and the posting of private photos without consent. TFVAW in India occurs in the form of many online harms that disproportionately affect women. These include doxxing of personal information, sextortion, deepfake pornography, coordinated trolling and abusive campaigns on social media, cyberstalking through persistent messaging, and financial scams that take advantage of trust through phishing or fraudulent investment schemes on digital platforms.[9]

Online violence takes many forms, including cyberstalking, relentless trolling and harassment, doxxing, non-consensual sharing of private photographs, sextortion, deepfake pornography, and cyber-flashing. Phishing, fraudulent investment schemes, or UPI fraud masquerading as romantic advances are common financial scams that target women. These schemes take use of trust and financial ignorance to exhaust savings or compel additional cooperation.[10]

This form of violence leverages the internet's anonymity, scalability and persistence to amplify traditional patriarchal harms and unprecedented ways. NCRB (National Crime Research Bureau) data reveals a sharp escalation, with cybercrime complaints against women rising form 10,730 case in 2021 to 14,409 in 2022.[11]

Despite its potential for empowerment, technology frequently makes gender inequality worse by creating structural, social, and operational disadvantages that disproportionately affect women. These show up as obstacles to entry, increased susceptibility to mistreatment. Here are a few drawbacks:

- Digital gender divide: Women have 20-30% lower internet access and device ownership than men, limiting education, jobs and financial independence

- Low digital literacy: Compared to 41% of males, just 21% of Indian women have basic digital abilities, making them dependent on male family members to do internet activities.

[8] UN Women, *Model Framework for Legislation on Technology-Facilitated Violence Against Women and Girls* 12–15 (2025).
[9] International Center for Research on Women, Technology-Facilitated Gender-Based Violence in India 23–28 (2021).
[10] Equality Now, *Experiencing Technology-Facilitated Gender-Based Violence in India* 30–35 (2025).
[11] National Crime Records Bureau, *Crime in India 2022*, vol. 2, at 156–162 (2023).

- Content virality: Abusive content spreads quickly over networks and is impossible to completely remove, permanently harming one's reputation.

- Financial targeting: Romance scams and UPI fraud take advantage of women's relative inexperience, resulting in disproportionate financial loss.

- Deepfake pornography: AI programs weaponize women's photos by producing non-consensual sexual content from any image.

- Evidentiary volatility: Digital evidence disappears or gets altered, frustrating legal prosecution

Legal Provisions and Judicial Framework

In the face of growing cyberthreats, India's legal response to violence against women enabled by technology has gradually changed from constitutional underpinnings to specialized cyber provisions.[12] The Constitution's Articles 14, 15, 19, and 21 provide equality, non-discrimination, and protections for life, liberty, privacy, and dignity. These rights have gradually been extended to virtual realms through court interpretation, most notably when Puttaswamy (2017) affirmed informational privacy.[13]

Through specific statutes, this normative foundation is operationalized. Sections 66C (identity theft), 66E (privacy violation), 67 (obscene material), 67A (sexually explicit content), and 67B (child pornography) of the Information Technology Act 2000, which was passed during the early growth of the internet, specifically addressed online harassment, non-consensual image sharing, and cyberstalking as digital age extensions of traditional harms.[14]

The Bharatiya Nyaya Sanhita 2023 modernized criminal law by renaming IPC offenses as Sections 79 (sexual harassment), 77 (voyeurism), 78 (stalking), 351 (criminal intimidation), and 74 (insult to modesty), which are clearly relevant to technology-mediated conduct.[15]

Through significant examples, judicial growth became very clear. Cyber harassment liability

[12] Press Information Bureau, Cybercrime Against Women (Oct. 27, 2022).
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India); INDIA CONST. arts. 14, 15, 19, 21.*
[14] Information Technology Act, No. 21 of 2000, §§ 66C, 66E, 67, 67A, 67B (India)..
[15] Bharatiya Nyaya Sanhita, No. 45 of 2023, ss 74, 77, 78, 79, 351 (India).

was established in State of Tamil Nadu v. Suhas Katti (2004), which was the first conviction under the IT Act for pornographic emails directed at a woman.[16] The framework was improved in Shreya Singhal v. Union of India (2015), which upheld targeted remedies while overturning Section 66A's excessive scope.[17]

Although this development is consistent with adaptive jurisprudence, its ability to combat the anonymity and scope of technology calls for careful consideration.

Persistent Challenges in Implementation

Despite this changing legal framework, women who are victims of abuse enabled by technology face significant practical obstacles that compromise legal protections. Due to widespread stigma, victim blaming, and fear of reputational escalation through judicial disclosure, only a small percentage of occurrences reach formal channels, according to NCRB data. Underreporting is still widespread.[18]

The issue is made worse by institutional flaws. Police frequently lack specialized cyber forensics training, which can result in improper handling of digital evidence, delayed requests for server data, and jurisdictional problems when offenders operate internationally or across state lines. Because first answers prioritize moralistic questioning above offender accountability, procedural insensitivity further deters survivors.[19]

Vulnerabilities are made worse by poor platform governance. While grievance procedures are delayed, unclear, or inaccessible due to language barriers, intermediaries utilize uneven moderation algorithms that fail to identify gendered harassment. Anonymous accounts avoid identification, and content virality guarantees that harmful content endures beyond removal orders.[20]

Legislative blind spots are revealed by emerging concerns like deepfakes and AI-generated pornography, while current laws struggle with new kinds of evidence. Institutional will and

[16] *State of Tamil Nadu v. Suhas Katti, Cyber Crime Case No. 4680 of 2004 (Mahila Ct., Chennai).*
[17] *Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).*
[18] National Crime Records Bureau, *Crime in India 2022*, vol. 2, at 158 (2023).
[19] Samridhi Goyal, Cyber Crimes against Women and Prevention, 15–18 (Chanakya Nat'l L. Univ. 2025).
[20] IT for Change, *Technology-Mediated Violence Against Women in India: A Review* 40–45 (2017).

community support are further undermined by sociocultural norms that trivialize online damages as "virtual" rather than real.[21]

These interrelated legal, technical, institutional, and normative barriers turn theoretical protections into real-world illusions, necessitating a reassessment of whether India's system actually mitigates the gendered drawbacks of technology.[22]

Recommendations for Effective Reform

Targeted, multi-layered reforms are necessary to bridge these implementation gaps and turn theoretical rights into real-world safeguards for women. In addition to victim-centric practices like in-camera trials, expedited cyber courts, and obligatory compensation funds, legislative criminalization of new dangers like deepfake pornography, sextortion, and coordinated online gender abuse would clarify prosecutorial routes.[23]

Establishing district-level specialized Women Cyber Protection Units with gender-sensitive protocols and forensic training would expedite investigations. Evidentiary delays could be decreased by requiring real-time server data access for platforms and integrating the National Cyber Crime Reporting Portal with local law enforcement and legal aid organizations.

AI-driven proactive detection of non-consensual intimate imagery, multilingual one-click reporting tools, 24-hour removal promises for gendered abuse, and yearly transparency reports broken down by victim gender are all examples of the increased due diligence that platforms must provide. Intermediary responsibility rules should impose progressive penalties for noncompliance.

Resilience could be prevented through community awareness campaigns on legal remedies, national computer literacy programs aimed at women and girls, and collaborations with NGOs to support survivors. These interrelated strategies (doctrinal accuracy, institutional capacity, platform accountability, and empowerment initiatives) offer a thorough strategy to counteract

[21] Equality Now, *Experiencing Technology-Facilitated Gender-Based Violence in India* 45–50 (2025).
[22] LawGratis, Challenges to Indian Law and Cyber Crime Scenario in India (July 17, 2025).
[23] UN Women, *Model Framework for Legislation on Technology-Facilitated Violence Against Women and Girls* 50–55 (2025).

the gendered drawbacks of technology while utilizing its liberating promise.[24]

Conclusion: Towards Gender-Just Digital Spaces

This analysis highlights the deep ambivalence of technology for Indian women: while it is hailed as a catalyst for empowerment, it also perpetuates disadvantages through institutional inertia, restrictive access, and increased abuse.[25] Cyberstalking, deepfakes, financial frauds, and online violence all take advantage of platform architecture to maintain patriarchal control, and NCRB statistics highlight their growing frequency in the face of insufficient protections.[26]

India's legal development shows doctrinal flexibility, from judicial clarifications in Suhas Katti and Shreya Singhal to constitutional privacy guarantees through IT Act provisions.[27] However, ongoing issues, underreporting, forensic shortcomings, platform opacity, and normative trivialization reveal a crucial gap between the written legislation and practical remedies.

To close this gap, the advanced recommendations incorporate preventive literacy, platform accountability, institutional fortification, and doctrinal accuracy. In order to achieve true reform, "Digital India" must be measured by women's unrestricted, respectable involvement in virtual spaces rather than just connectivity numbers.[28]

In the end, the gendered drawbacks of technology put constitutional guarantees of equality and dignity to the test. The infrastructure for protection is found in India's legal-judicial system, but realizing it need for swift, concerted effort. Then and only then can women be empowered by digital advancement rather than put in danger, turning potential risk into real opportunity. Frameworks spotlighting equal digital citizenship must take precedence above the shadows of online exploitation.

India's legal system is prepared to face the gendered shadows of technology, but women's path to digital equality will only be illuminated by determined execution. This assessment urges

[24] International Center for Research on Women, *Technology-Facilitated Gender-Based Violence in India* 40–45 (2021).
[25] UN Women, *Model Framework for Legislation on Technology-Facilitated Violence Against Women and Girls* (2025).
[26] National Crime Records Bureau, *Crime in India 2022*, vol. 2, Cyber Crimes Against Women (2023).
[27] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[28] International Center for Research on Women, *Technology-Facilitated Gender-Based Violence in India: Key Trends and Responses* (2021).

immediate action to ensure that technology empowers rather than threatens, transforming safeguards from paper promises into actual protections.