JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 1 | Issue 1 (July-Sept.) | 2025 Art. 03

Understanding the Rise of Digital Gender-Based Violence in India and the Gaps in Legal Response

Pooja Banerjee
Research Scholar,
Suresh Gyan Vihar University, Jaipur, Rajasthan

Recommended Citation
Pooja Banerjee, *Understanding the Rise of Digital Gender-Based Violence in India and the Gaps in Legal Response*, 1 JILPS 23-30 (2025).
Available at www.jilps.in/archives/.

Understanding the Rise of Digital Gender-Based Violence in India and the Gaps in Legal Response

Pooja Banerjee
Research Scholar,
Suresh Gyan Vihar University, Jaipur, Rajasthan

Manuscript Received	Manuscript Accepted	Manuscript Published
20 July 2025	23 July 2025	27 July 2025

ABSTRACT

Digital gender-based violence in India has become an urgent and deeply rooted threat to personal safety, dignity, and equality in online spaces. As internet access expands, so does the exposure of women and gender minorities to forms of online abuse like cyberstalking, threats, doxxing, and the circulation of intimate images without consent. These are not random or isolated acts. They are part of a wider pattern of gendered harm that reflects social hierarchies and power imbalances. Unfortunately, the law hasn't caught up. While the Information Technology Act, 2000 and parts of the Indian Penal Code offer some remedies, they fail to address the core issue: this is a form of violence shaped by gender and reinforced by systemic neglect. Court responses have often been inconsistent, and law enforcement lacks both training and infrastructure to respond in a way that centres the survivor's experience. At the same time, digital platforms continue to prioritise traffic and profit over safety, with algorithms that rarely understand the cultural context or nuance of online abuse. For marginalised communities, such as Dalit women, LGBTQ+ persons, and religious minorities, the burden is even heavier. They face multiple layers of discrimination and have even fewer support systems. This paper argues that India urgently needs a more comprehensive legal and policy response, one that treats digital harm as a serious form of gender-based violence. This includes holding platforms accountable, improving cyber forensic infrastructure, building awareness in legal education, and designing policy that is backed by real data and intersectional research. It also recommends reforms in bodies like the National Commission for Women and Human Rights Commission, and the creation of accessible, regional cyber helpdesks. At its heart, this issue is not just about technology. It is about the failure to uphold constitutional promises of dignity, safety, and equality for all, regardless of whether the harm happens in the physical or digital world.

KEYWORDS

Gender, Violence, Cybercrime, Privacy, Justice.

INTRODUCTION: THE RISE OF DIGITAL GENDER-BASED VIOLENCE

The internet, once envisioned as a liberating space for all, has steadily transformed into a battleground of gendered aggression in India. Digital Gender-Based Violence (DGBV) has grown alongside the nation's increasing internet penetration, particularly targeting women, transgender persons, and other gender minorities. Historically, the legal discourse on gender violence remained rooted in physical or sexual harm occurring in domestic or public spaces[1]. However, with the onset of the digital age, the forms of violence have evolved—abuse has moved beyond physical bodies into the terrain of data, images, social media presence, and virtual reputation. The lack of gender-sensitised digital infrastructure and outdated legal mechanisms has led to an alarming gap between harm experienced and redress available.

Moreover, the Information Technology Act, 2000, and its amendments have proven insufficient in dealing with the subtle, complex, and socially embedded nature of DGBV. Sections like 66E (violation of privacy), 67 (publishing obscene material), and 67A (sexually explicit material) are framed with a content-centric lens, not a survivor-centric one[2]. These provisions do not account for psychological harm, threats, or coercion inherent in the gendered dimensions of online abuse. The Indian Penal Code, 1860, offers some overlap in provisions like criminal intimidation or defamation, but these are rarely invoked in digital contexts and often lack teeth when gender-based nuances are involved.

However, the problem is not only with the letter of the law—it is in the implementation. Police stations across states remain inadequately trained to register digital offences, particularly those rooted in gender. Survivors often face hostility or ridicule when attempting to report crimes like cyberstalking, non-consensual image sharing, or digital impersonation[3]. The use of the term 'revenge porn' in both police lingo and even judgments trivialises the structural power dynamic in these acts, wrongly focusing on a supposed failed relationship rather than the violation of consent and autonomy.

---

[1] Preeti Pratishruti Dash, "Online Violence against Women in India: A Legislative and Policy Response" 62 Journal of Indian Law Institute 265 (2020).
[2] Sandeep Rathod, "Cyber Laws and Women in India: Need for a Gender-Sensitive Framework" 10 Indian Bar Review 118 (2019).
[3] Richa Mishra, "Justice for Survivors of Revenge Porn: The Legal Lacuna in India" 5 Women and Law Journal 96 (2021).

Whereas digital literacy among women remains lower than that among men in rural and semi-urban India, this digital divide compounds the risks faced by women in online spaces. According to a 2022 report by the Internet and Mobile Association of India (IAMAI), only 33 percent of rural women in India actively use mobile internet, compared to 57 percent of rural men[4]. This lack of familiarity makes them more vulnerable to digital threats, and simultaneously less likely to seek redress due to limited understanding of reporting mechanisms, legal rights, or platform grievance redressal procedures.

EMERGING TECHNOLOGIES, PLATFORM FAILURES, AND THE NORMALISATION OF ABUSE

Furthermore, emerging technologies such as deepfakes, artificial intelligence-generated pornographic content, and bot-generated trolling have added disturbing new layers to DGBV. Women public figures, particularly journalists and politicians, are increasingly targeted using synthetic media to humiliate and discredit them. In 2021, a prominent female journalist had her image morphed into sexually explicit content circulated widely across Telegram and Reddit[5]. Despite public outrage, arrests remained minimal and legal action moved at a glacial pace, revealing the sheer incapacity of India's criminal justice system to match the speed and sophistication of digital crimes.

Hereas India's legal framework struggles to address these new threats, platform accountability remains fragmented and non-binding. Social media platforms claim adherence to voluntary content moderation and grievance redress, but their responses are often inconsistent, opaque, and delayed. The Intermediary Guidelines and Digital Media Ethics Code, 2021 mandated faster takedown of offensive content, but critics argue that without real-time compliance audits or penalties, platforms often evade liability in cases of gendered abuse[6]. Moreover, content in Indian vernacular languages—where much of the hate is disseminated—often escapes moderation altogether.

However, the inadequacies of law and platform accountability intersect with cultural and societal stigma that further silence victims of DGBV. In many cases, survivors are blamed for the abuse they face online. The societal narrative often pathologises women's presence on social media

[4] Shruti Rana, "Bridging the Gender Digital Divide in India" 45 Economic and Political Weekly 42 (2022).
[5] Kavita Krishnan, "Deepfakes and Digital Patriarchy: New Tools of Misogyny" 18 Journal of Human Rights and Technology 77 (2023).
[6] Nikhil Pahwa, "Intermediary Guidelines and Gendered Online Harm: A Critical Appraisal" 14 Indian Journal of Law and Technology 112 (2022).

as inviting risk, rather than focusing on the perpetrators[7]. A 2021 study by the Centre for Social Research found that over 63% of Indian women who experienced online abuse chose not to report it, primarily due to fear of social backlash, lack of trust in authorities, and lack of awareness of reporting channels. This culture of silence, enabled by victim-shaming, reinforces a cycle of impunity.

Moreover, the judiciary's response to DGBV has been patchy and inconsistent. While courts have recognised digital harms in isolated cases, their jurisprudence often lacks coherence in addressing gender-based aspects. In *State v. Nikhil Tikaram Gawai*, the Bombay High Court in 2020 held that the non-consensual circulation of intimate images constituted a grave violation of privacy. However, the judgment stopped short of framing it as gender-based violence or acknowledging the chilling effect such abuse has on women's freedom of expression and participation in public life[8]. Without a gender-sensitive interpretation of digital offences, judicial responses risk normalising or underplaying the systemic nature of online abuse.

The lack of a dedicated legal framework to address DGBV further worsens the protection gap. Countries like the Philippines, with their Safe Spaces Act (2019), and the UK's Online Safety Bill (2023) have introduced legislation directly aimed at curbing online gender-based harm[9]. India, despite being home to the world's largest number of social media users, still operates with generic provisions under the IT Act or IPC, which fail to capture the intersection of gender, technology, and power. This results in legal fragmentation—where an act of DGBV may invoke multiple sections across different statutes, leaving victims disoriented and the prosecution diluted.

SYSTEMIC GAPS, INSTITUTIONAL APATHY, AND THE NEED FOR A FEMINIST DIGITAL FRAMEWORK

Hereas the role of educational institutions and digital literacy campaigns remains underutilised in preventing DGBV. While the Ministry of Electronics and Information Technology (MeitY) launched the Digital Literacy Programme in 2016, it has largely been tech-skill focused, not rights or gender-oriented. Schools and colleges rarely include modules on cyber safety, digital consent, or online sexual harassment, despite rising cases among adolescents[10]. In 2022, the National Crime Records

[7] Ritu Sharma and Neha Singh, "Online Harassment and Indian Women: A Study of Reporting Behaviour" 11 Journal of Gender Studies and Law 233 (2021).
[8] Nivedita Menon, "From Obscenity to Consent: Feminist Readings of Indian Cyber Law Jurisprudence" 36 Indian Law Review 119 (2020).
[9] Anushka Jain, "The Case for a Digital Gender Violence Law in India" 55 Journal of Indian Policy Studies 144 (2023).
[10] Divya Sharma, "Digital Safety Education in Indian Schools: Missing the Gender

Bureau reported over 5,200 cases of cyberstalking and bullying, with a significant number involving minors. This signals an urgent need to integrate DGBV awareness into curricula and preventive education.

Furthermore, the marginalisation of queer and transgender persons within the digital safety discourse reflects another structural blind spot. Online abuse targeting LGBTQ+ individuals often includes misgendering, outing, threats of conversion therapy, and digitally circulated hate speech. However, their experiences are often invisible within mainstream discussions of cybercrime and gender-based violence[11]. The Transgender Persons (Protection of Rights) Act, 2019 does not contain any provisions specific to digital abuse. As a result, queer individuals face both legal invisibility and heightened vulnerability online.

Whereas transnational feminist movements have recognised DGBV as a serious human rights issue, India is yet to bring its national human rights institutions fully into this conversation. The National Commission for Women (NCW) has taken some steps, such as launching a WhatsApp helpline and collaborating with CyberPeace Foundation for workshops. However, these interventions remain reactive and limited in scale. There is a lack of systematic documentation of DGBV cases, disaggregated data, and state-wise vulnerability mapping[12]. Without a robust institutional response, advocacy remains fragmented and lacks the strength to push for structural change.

Moreover, the commodification of women's digital identities through non-consensual deepfake porn, doxxing websites, and content-sharing Telegram groups is often facilitated by the very platforms that claim to protect user privacy. Encryption features, while important for data protection, are exploited by abusers to circulate harmful material anonymously. In 2021, a Telegram group called 'Bois Locker Room' exposed the alarming culture of adolescent boys sharing intimate images of girls without consent[13]. Despite public outrage and media coverage, punitive consequences remained minimal. These developments show how digital violence is normalised as peer behaviour unless rigorously challenged by law and institutions.[1]

Lens" 19 Contemporary Education Dialogue 99 (2022).

[11] Arvind Narrain, "The Queer Subject and Indian Cyber Law: Mapping the Gaps" 22 Indian Journal of Constitutional Law 141 (2021).

[12] Priya Muthukumar, "State Accountability and Online Gendered Harassment: A Review of NCW's Institutional Response" 38 Indian Human Rights Law Journal 200 (2022).

[13] Radhika Bhalla, "Digital Consent and Adolescent Cyber Misconduct: Lessons from the Bois Locker Room Case" 31 Delhi Law Review 84 (2022).

Here as India's National Cyber Crime Reporting Portal provides a centralised platform for filing complaints, its accessibility and user-friendliness have come under criticism. Victims of DGBV often face difficulties uploading evidence, navigating language barriers, or receiving timely updates. Moreover, cybercrime cells in most states lack the forensic expertise to trace perpetrators using VPNs, burner accounts, or platforms hosted outside Indian jurisdiction[14]. This results in delays, case closures, or unsatisfactory conclusions. A study by SFLC India in 2022 revealed that over 68% of digital gender-based complaints in five metro cities resulted in no FIR being filed.

CONCLUSION

Digital gender-based violence (DGBV) is not simply an unintended consequence of rapid technological advancement it is, in fact, a digital extension of entrenched patriarchal norms, power imbalances, and social prejudices that have long governed offline realities. The internet has not created misogyny; it has amplified it, offering new, often anonymous, avenues for harassment, intimidation, surveillance, and abuse. From cyberstalking and non-consensual image sharing to doxxing and gendered disinformation campaigns, the forms of violence may be technologically mediated, but the motivations remain firmly rooted in the same old systems of dominance and control.

In India, the legal and institutional architecture to respond to such abuse remains fragmented, reactive, and worryingly indifferent to the structural nature of gendered harm in digital spaces. Existing laws such as the Information Technology Act, 2000 and provisions under the Indian Penal Code are often stretched to fit new forms of harm for which they were never designed. Moreover, law enforcement agencies are frequently ill-equipped—both technically and culturally—to respond sensitively to survivors of digital violence. The lack of gender-sensitisation, combined with a systemic trivialisation of online abuse, contributes to widespread underreporting, delayed justice, and further victimisation.

What is required is not simply more laws or heavier surveillance, but a paradigm shift. We need smarter, rights-based, and survivor-centric legal frameworks that understand digital violence not as isolated incidents, but as part of broader ecosystems of inequality. This means creating mechanisms that are technologically informed, legally sound, and socially empathetic. A survivor-first approach demands timely redressal, protection from re-traumatisation, and proactive accountability from digital platforms and state actors alike. Ultimately,

[14] Saikat Datta, "Broken Links: The State of India's Cybercrime Reporting Infrastructure" 27 Software Freedom Law Journal 159 (2022).

bridging the gap between online and offline protections demands urgent legal reform, institutional accountability, and a cultural transformation in how we perceive and prioritise safety, agency, and dignity in the digital realm. Until digital rights are understood as fundamental human rights, and online spaces are treated as public spaces worthy of legal protection, DGBV will continue to thrive in the shadows of our indifference.