

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Protection of Women on Social Media Platforms in India: A Critical Analysis of Legal Remedies and Regulatory Mechanisms

AKILA C*

ABSTRACT

The exponential proliferation of social media platforms in India has democratized digital expression, yet it has simultaneously exposed women to severe forms of gender-based cyber violence. Offences such as cyberstalking, the non-consensual sharing of intimate images, deepfake generation, doxing, and online harassment severely undermine female autonomy and digital safety. This paper critically analyses the structural efficacy of the existing legal remedies and regulatory frameworks designed to protect women on social media platforms in India. It evaluates statutory provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (BNS), and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Through a socio-legal qualitative analysis, the research assesses the operational challenges faced by victims, including delayed takedowns, jurisdictional bottlenecks, loopholes in intermediary immunity, and policing biases. The findings indicate that while legislative instruments have evolved to recognize new vectors of digital harm, implementation remains significantly constrained by inadequate police capacity, poor algorithmic accountability on the part of platforms, and the social stigma that deters reporting. The paper argues for comprehensive structural reforms, including strict enforcement of intermediary grievance timelines, specialized digital police cells, mandatory content moderation standards, and enhanced digital literacy initiatives, to foster a safer online ecosystem for women.

Keywords: Social Media, Women's Cyber Safety, Cyber Violence, Cyberstalking, Non-Consensual Intimate Images, Deepfakes, Doxing, Online Harassment, Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Intermediary Guidelines, Digital Rights, Content Moderation, Legal Remedies, Digital Literacy

I. INTRODUCTION

The rise of digital technology and widespread internet access across India have fundamentally transformed human communication, governance, and commerce. Social media platforms such

* Author is a Student at S. Thangapazham Law College, Vasudevanallur, Tenkasi, Tamil Nadu, India.

as Instagram, X, Facebook, and WhatsApp have given women unprecedented opportunities for public engagement, economic independence, and socio-political expression. This virtual expansion, however, has been shadowed by a parallel rise in gender-based cyber violence.¹ Online spaces often replicate and amplify offline patriarchal power structures, creating a hostile digital environment in which women are disproportionately targeted with misogynistic abuse, harassment, and violations of privacy.

The nature of digital harm differs significantly from that of physical offences because of the viral, permanent, and boundaryless nature of the internet. A single shared image or defamatory post can circulate indefinitely across multiple platforms, inflicting continuing psychological, social, and professional damage on the victim. Recognizing these threats, the Indian legal system has attempted to adapt its regulatory architecture. Legislative efforts range from penal statutes targeting specific digital crimes to administrative rules imposing duties on social media intermediaries.

Despite these statutory developments, the practical enforcement of digital safety for women remains problematic. Victims frequently encounter institutional apathy, convoluted grievance mechanisms, delayed content removal, and significant delays in legal proceedings. Furthermore, the rapid advancement of artificial intelligence, particularly deepfake technology, presents novel regulatory hurdles that traditional laws were not designed to handle. This paper critically evaluates the existing legal, institutional, and platform-driven mechanisms intended to protect women on social media platforms in India, identifies the key lacunae, and proposes reforms.

II. REVIEW OF LITERATURE

Legal scholars and cyber law experts have increasingly highlighted the intersection between digital technology, constitutional rights, and gender violence in India. The cyber law expert Pavan Duggal emphasizes that while the Information Technology Act, 2000 was initially aimed at facilitating e-commerce, subsequent amendments were compelled to address cybercrimes against individuals.² Researchers point out, however, that statutory language often struggles to capture the nuanced realities of online gender-based abuse. Early penal provisions, for instance, relied heavily on outdated standards of “obscenity” rather than on victim consent and bodily autonomy.³

¹ See NATIONAL CRIME RECORDS BUREAU, MINISTRY OF HOME AFFAIRS, CRIME IN INDIA 2022 (2023).

² PAVAN DUGGAL, CYBERLAW: THE INDIAN PERSPECTIVE (3d ed. 2009).

³ See generally DEBARATI HALDER & K. JAISHANKAR, CYBER CRIME AND THE VICTIMIZATION OF WOMEN: LAWS, RIGHTS AND REGULATIONS (2012), <https://doi.org/10.4018/978-1-60960-830-9>.

Contemporary socio-legal literature treats digital violence as an extension of structural patriarchy. Research by organizations such as Amnesty International has documented the chilling effect of online abuse on women in public life, demonstrating that targeted harassment operates as a tool of silencing and censorship.⁴ Studies analyzing intermediary liability argue that platforms often hide behind “safe harbor” protections, treating content moderation as a secondary concern rather than a fundamental duty of care. Empirical studies of law enforcement responses likewise reveal substantial gaps between legislative intent and ground reality. Researchers observe that local police personnel frequently lack technical training in digital forensics, which leads to improper evidence collection and the mishandling of electronic records. Literature on the Information Technology Rules, 2021 notes that although strict timelines were introduced for content removal, enforcement remains inconsistent, and international platforms often delay compliance with domestic law enforcement requests.⁵

III. OBJECTIVES

The primary objectives of this study are as follows:

- To evaluate the statutory and penal protections available to women against online abuse under the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000.
- To critically analyse the regulatory framework governing social media intermediaries, specifically examining the efficacy of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- To identify the procedural, institutional, and technological obstacles encountered by women when reporting cybercrimes and seeking legal remedies.
- To examine the emerging challenge of synthetic media, deepfakes, and algorithmic bias in targeted abuse against women.
- To formulate policy recommendations and regulatory suggestions aimed at enhancing judicial efficiency, platform accountability, and victim support systems.

IV. METHODOLOGY AND DATABASE USED

This study adopts a qualitative, doctrinal, socio-legal research methodology. The inquiry is grounded in the critical analysis of legal statutes, legislative instruments, judicial precedents,

⁴ AMNESTY INTERNATIONAL, *Toxic Twitter: Violence and Abuse Against Women Online*, AI Index ACT 30/8070/2018 (Mar. 2018), <https://www.amnesty.org/en/documents/act30/8070/2018/en/>.

⁵ See Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India).

and institutional reports governing cybercrimes against women in India. The study evaluates primary legal sources alongside secondary literature to examine the gap between legal theory and practical enforcement.⁶ The database used for this research comprises the Bharatiya Nyaya Sanhita, 2023 (BNS); the Information Technology Act, 2000 (and its 2008 amendment); and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.⁷ Key judgments of the Supreme Court of India and various High Courts on digital privacy, intermediary liability, obscenity, and cyber harassment are also considered.⁸

V. STATUTORY PENAL REMEDIES UNDER INDIAN LAW

The penal architecture addressing cybercrimes against women is divided primarily between general criminal law and specialized digital legislation. Under the Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, 1860, specific provisions address conduct that violates women's privacy and dignity. Key offences include stalking, including the monitoring of a woman's electronic communications (Section 78); voyeurism, including the dissemination of images of a woman engaged in a private act (Section 77); and any word, gesture or act intended to insult the modesty of a woman (Section 79). Provisions on criminal intimidation and defamation may also apply.⁹

Complementing the penal code, the Information Technology Act, 2000 contains dedicated provisions for cyber-specific violations. Section 66E criminalizes the intentional violation of privacy by capturing, publishing, or transmitting the image of a private area of a person without consent. Sections 67 and 67A penalize the publication or transmission of obscene and sexually explicit material in electronic form. Despite these statutory tools, enforcement often falters because of overlapping provisions and the procedural requirements governing electronic evidence, which can prolong prosecution and delay immediate relief for victims.¹⁰

⁶ LEGAL RESEARCH AND METHODOLOGY (S.N. Jain, J.K. Mittal, Kusum & P. Kalpakam eds., 1983).

⁷ The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India); The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India).

⁸ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, AIR 2015 SC 1523 (India); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

⁹ The Bharatiya Nyaya Sanhita, 2023, §§ 77–79, No. 45, Acts of Parliament, 2023 (India); *see also id.* §§ 351 (criminal intimidation), 356 (defamation).

¹⁰ The Information Technology Act, 2000, §§ 66E, 67, 67A, No. 21, Acts of Parliament, 2000 (India); *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India) (construing section 65B of the Indian Evidence Act, 1872, whose counterpart is now section 63 of the Bharatiya Sakshya Adhiniyam, 2023).

VI. REGULATORY DUTIES OF INTERMEDIARIES UNDER THE IT RULES, 2021

Social media platforms operate as “intermediaries” under Section 2(1)(w) of the Information Technology Act, 2000. Section 79 grants them conditional immunity from liability for third-party content, subject to compliance with the statutory requirements and the due diligence framework.¹¹ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 significantly strengthened these obligations, particularly for significant social media intermediaries.

The Rules introduced specific protections for women, including an obligation to remove or disable access, within the prescribed period, to certain intimate, sexually explicit, impersonating, or private content on receipt of a complaint. The Rules also require significant social media intermediaries to appoint designated compliance and grievance officers.¹² While these provisions represent a positive regulatory shift toward victim-centric relief, platforms frequently rely on automated moderation systems that may fail to understand regional Indian languages, cultural nuances, and contextual abuse. Consequently, some grievances may be inadequately addressed, requiring victims to pursue further grievance mechanisms and appeals while the harmful content continues to circulate.

VII. EMERGENCE OF DEEPPAKES AND SYNTHETIC MEDIA THREATS

The rapid advancement and accessibility of artificial intelligence tools have created new mechanisms of digital abuse, most notably synthetic media and deepfakes. Deepfake technology allows perpetrators to superimpose a woman’s face onto sexually explicit media, or to create realistic audio-visual fabrications, without her knowledge or consent. This form of targeted abuse threatens female public figures, journalists, students, and private individuals alike, with serious reputational and psychological consequences.¹³

The existing legal system faces conceptual challenges in prosecuting deepfake offences effectively. Although provisions concerning forgery, defamation, privacy, and offences against the dignity of women may apply depending on the facts, the IT Act contains no single comprehensive offence designed for every form of AI-generated deepfake abuse.¹⁴ Furthermore,

¹¹ The Information Technology Act, 2000, §§ 2(1)(w), 79, No. 21, Acts of Parliament, 2000 (India).

¹² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–4, G.S.R. 139(E) (Feb. 25, 2021) (India).

¹³ *See id.* r. 3(2)(b) (requiring an intermediary, on a complaint made by or on behalf of the individual concerned, to remove or disable access to content that prima facie exposes that individual’s private area, shows the individual in full or partial nudity or in a sexual act or conduct, or is in the nature of impersonation in electronic form, including artificially morphed images of the individual).

¹⁴ *See* The Bharatiya Nyaya Sanhita, 2023, §§ 79, 336, 356, No. 45, Acts of Parliament, 2023 (India); The Information Technology Act, 2000, §§ 66E, 67, 67A, No. 21, Acts of Parliament, 2000 (India).

attributing authorship of a deepfake can be technically complex, because perpetrators may use anonymous accounts, VPNs, foreign platforms, and decentralized tools.

VIII. PROCEDURAL CONSTRAINTS IN POLICE INVESTIGATION AND FORENSICS

The path toward legal redress for online abuse is fraught with procedural hurdles for women victims. Reporting a cybercrime may begin at a police station or through the National Cyber Crime Reporting Portal.¹⁵ However, deficiencies in technical competence, gender sensitivity, and understanding of digital gender-based violence can affect the reporting and investigation process. Victims may also face insensitive questioning about their online conduct, which can discourage them from pursuing formal complaints.

From an investigative standpoint, cybercrime investigation requires the timely preservation and examination of digital evidence, including metadata, logs, device information, and other relevant forensic material.¹⁶ Police forces in some jurisdictions face inadequate digital forensic infrastructure and backlogs in forensic laboratories. Furthermore, where the relevant data is held by foreign service providers, obtaining subscriber information and other records may involve formal international cooperation mechanisms and lengthy correspondence, delaying investigations.

IX. JURISDICTIONAL COMPLEXITIES AND CORPORATE ACCOUNTABILITY

The global nature of the internet fundamentally conflicts with the territorial boundaries of national law enforcement.¹⁷ Social media companies operate across international borders, and relevant information may be stored on cloud servers located in multiple jurisdictions. When an offence occurs within India, obtaining cooperation from overseas service providers can create legal and procedural difficulties involving privacy, jurisdiction, and international cooperation.

Moreover, commercial interests may conflict with human rights obligations. Social media business models frequently depend on user engagement, while algorithms may amplify sensational, controversial, or highly engaging content. Although Indian regulatory directives seek to promote platform accountability, balancing fundamental rights such as the freedom of

¹⁵ MINISTRY OF HOME AFFAIRS, GOVERNMENT OF INDIA, *National Cyber Crime Reporting Portal*.

¹⁶ See The Bharatiya Sakshya Adhiniyam, 2023, §§ 61–63, No. 47, Acts of Parliament, 2023 (India) (governing the admissibility of electronic and digital records).

¹⁷ See The Information Technology Act, 2000, § 75, No. 21, Acts of Parliament, 2000 (India) (extending the Act to offences and contraventions committed outside India that involve a computer, computer system or computer network located in India).

speech under Article 19(1)(a) and the right to privacy under Article 21 against the regulatory obligations imposed on platforms remains a significant constitutional and legal challenge.¹⁸

X. SUGGESTIONS

1. **Enacting statutory amendments.** To address the systemic bottlenecks and regulatory gaps in protecting women on social media platforms, statutory amendments must be enacted to define and penalize explicitly emerging digital harms such as deepfakes, AI-generated synthetic media, doxing, and non-consensual digital manipulation.
2. **Legislative modernization.** The legislative framework requires modernization to move beyond traditional definitions of obscenity and to focus instead on consent, privacy, and bodily autonomy.
3. **Framing of regulations.** Regulatory authorities must mandate higher standards of content moderation for social media intermediaries, requiring platforms to invest in localized, human content moderation infrastructure that understands regional Indian languages, colloquialisms, and socio-cultural contexts, and so reducing sole reliance on automated algorithms that routinely misinterpret targeted gender abuse. Social media corporations should also be required to establish proactive detection mechanisms, such as automated digital hashing, to prevent the re-uploading of flagged viral media.
4. **Strengthening law enforcement.** At the institutional level, capacity building within law enforcement is essential to bridge the gap between statutory intent and on-ground enforcement. State governments should establish dedicated, specialized all-women cyber cells in every district, staffed with officers trained in digital forensics, cyber law, and gender-sensitive crisis response, to expedite the collection of digital evidence and eliminate moral policing.
5. **Responsibilities of law enforcement and policy.** Finally, long-term policy interventions must prioritize legal literacy, corporate cooperation, and fast-track adjudication, supported by streamlined cross-border data-sharing protocols established by the Ministry of Home Affairs and the Ministry of External Affairs to accelerate law enforcement requests sent to foreign-headquartered technology companies.

¹⁸ INDIA CONST. arts. 19(1)(a), 21; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

XI. CONCLUSIONS

The digital landscape holds immense potential for empowering women in India, but this potential cannot be fully realized while online spaces remain unsafe and hostile. The legal remedies and regulatory mechanisms currently operating in India provide a foundational structure, yet they exhibit critical operational gaps when confronted with modern cyber threats. Statutory provisions under the Bharatiya Nyaya Sanhita and the Information Technology Act offer formal avenues of justice, but systemic delays, forensic deficits, and patriarchal biases in law enforcement continue to impede access to timely relief.

Similarly, regulatory efforts under the IT Rules, 2021 have pushed social media intermediaries toward greater accountability, but the processes for removing non-consensual content remain insufficiently proactive. As AI-driven tools such as deepfakes democratize abusive capabilities, legislative frameworks must adapt proactively rather than reactively. Protecting women on social media platforms requires a holistic model that combines stringent legislative penalization, enforceable corporate accountability, rapid forensic infrastructure, and progressive societal change. Only through coordinated institutional action can the internet in India become an equitable, safe, and empowering space for women.
