VOLUME 7 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DIGITAL GENDER BASED VIOLENCE IN INDIA: A CRITICAL ANALYSIS ON THE STATUTORY GAPS AND REMEDIAL INADEQUACIES IN THE LEGAL REMEDIES

- Priya Veeresh Prabhu[1] & Suman Barman[2]

Abstract

Digital gender based violence has emerged as a critical threat to constitutional guaranties of privacy, dignity and bodily autonomy for women and gender marginalized individuals across India. Technology facilitated abuse has evolved from basic forms of electronic harassment into complex, systemic forms of gendered violence as internet access through mobile networks and digital platforms has rapidly expanded. These violations include non-consensual distribution of intimate images, doxxing, cyberstalking, online blackmail and artificial intelligence generated deep fakes. This paper provides a comprehensive doctrinal and socio-legal analysis of the legal structure governing digital gender based violence in India. Grounding its analytical framework in Article 21 of the Constitution of India, specifically the fundamental right to informational privacy and human dignity referred in Justice K.S. Puttaswamy v. Union of India, the study critically evaluates existing statutory mechanisms broadly as legal provisions, criminal codes and regulatory frameworks. This analysis examines major gaps in current legal remedies, including statutory, structural, and procedural issues. For example, Section 66E of the Information Technology Act focuses only on physical intimate body parts and does not address synthetic media, deep fake pornography, or AI-enabled identity manipulation. Other problems include procedural limits in digital evidence rules, forensic backlogs, slow content removal by platforms, and gender insensitivity among investigators, all of which make justice harder to achieve. The paper argues that handling digital violence only through criminalization or traditional obscenity

[1] Principal, Chembur Karnataka College of Law
[2] Assistant Professor at Chembur Karnataka College of Law

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

© 2026 International Journal of Advanced Legal Research

laws misses the core constitutional harm. To ensure safe and fair digital participation for everyone, the state needs a clear legal framework that defines synthetic media abuse, holds platforms accountable, improves forensic resources, and creates survivor-focused support systems based on digital dignity. The analysis reflects on the significant statutory, structural and procedural lacunae in current legal remedies. Specifically, key provisions such as Section 66E of the Information Technology Act focus narrowly on physical intimate body parts, failing to encompass synthetic media, deep fake pornography and AI enabled identity manipulation.

Moreover rules that govern evidence and digital evidence rules, big forensic backlogs, slow removal of content by platforms under intermediary rules and widespread gender bias, by investigators all block proper justice delivery. The paper signifies that looking at violence only with a fragmented criminal approach or old obscenity laws misconstrues the fundamental constitutional harm. Ultimately, to ensure safe and equitable digital participation for all citizens, the state requires a cohesive statutory framework that explicitly defines synthetic media abuse, enforces strict platform accountability, builds specialized forensic infrastructure and establishes survivor centric redressal mechanisms rooted in digital dignity.

Key words - Digital Gender-Based Violence, Cybercrime, Gender Justice, Statutory Gaps, Legal Remedies, Generative Artificial Intelligence, Deepfakes, Doxxing, Digital Privacy, Pl

Introduction

The rapid digital transformation of Indian society over the past decade has fundamentally restructured public and private communication[3]. The proliferation of low-cost smartphones, affordable high-speed mobile data and public digital infrastructure has brought hundreds of millions of citizens online. However, this democratic expansion of cyberspace has been accompanied by a parallel increase in technology-facilitated gender-based violence (DGBV). Far from being distinct from physical reality, digital spaces have become key arenas where structural gender inequalities, patriarchal norms and violence are reproduced, amplified and normalized.

[3] Loveleen Sharma & Suman Paliwal, "Gender Sensitivity in Cyberspace: A Doctrinal Analysis of Cybercrime and Gender Justice in India," 9(5) International Journal of Law Management & Humanities (2026), https://doi.org/10.63108/IJLMH.13038

© 2026 International Journal of Advanced Legal Research

Digital gender-based violence encompasses a broad spectrum of harmful behaviors carried out through electronic devices, social media platforms, messaging applications, and emerging digital environments. These behaviors include cyberstalking, non-consensual sharing of intimate images, doxxing, impersonation, coordinated online harassment, hate speech, and AI-driven image manipulation such as deepfakes. Rather than treating these acts as trivial digital inconveniences or minor criminal infractions, feminist legal theory and human rights frameworks increasingly recognize DGBV as a serious continuum of gender-based violence. The psychological distress, economic disruption, social ostracization, and self-censorship experienced by survivors demonstrate that digital harm inflicts severe real-world injury. While the Article 21[4], which guarantees the rights to life, personal liberty, privacy and human dignity, the translation of these constitutional ideals into effective statutory protection remains flawed. Current legislative instruments, primarily the Information Technology Act 2000[5] and the criminal codes updated under the Bharatiya Nyaya Sanhita (BNS) 2023[6], often fail to address the unique velocity, scale and anonymity that define online abuse.

Furthermore, the legal machinery experiences from severe operational constrainsts. The evidentiary requirements of digital forensics under the BNS[7], coupled with systemic delays in police investigations and compliance by social media platforms, leave victims with limited actionable recourse. As generative AI tools lower the technical barriers to the creation of non consensual synthetic media, emerging forms of digital violence are increasingly surpassing legal enforcement. This paper outlines a critical socio-legal analysis of digital gender-based violence in India. It begins by establishing the constitutional parameters of privacy, bodily autonomy, and human dignity in digital space. It then maps existing legal remedies in full statutory terms, identifying key gaps in criminal law, data protection law and intermediary regulation. The paper identifies procedural, forensic and institutional obstacles that survivors face in seeking justice. Finally, it proposes strategic policy recommendations and legislative reforms to develop a responsive and survivor-centric digital jurisprudence in India.

I. Constitutional Foundations

[4] The Constitution of India, art. 21
[5] The Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India)
[6] The Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India)
[7] *Ibid*

© 2026 International Journal of Advanced Legal Research

To understand the legal significance of the DGBV, the analysis needs to be incorporated within the Indian Constitutional framework. The Supreme court of India has been consistently broadened the definition of Article 21[8], evolving the guarantee of life and personal liberty into an extensive protection of human dignity, individual autonomy and bodily integrity. By targeting an individual's identification, privacy and public engagement, DGBV directly violates these constitutional safeguards.

The landmark nine-judge bench ruling in Justice K.S. Puttaswamy v. Union of India (2017)[9] is the cornerstone of contemporary Indian privacy jurisprudence. The right to privacy is an essential component of the right to life and personal liberty under Article 21[10], the Supreme Court ruled unanimously. Importantly, the court determined that privacy is a positive guaranty that safeguards individual autonomy, bodily integrity and informational privacy rather than just a negative right to be left alone. Justice D.Y. Chandrachud emphasized that privacy enables individuals to preserve their dignity and exercise control over their personal narrative.

Further, the constitutional liberties protected by Article 19(1)(a)[11] are restricted by DGBV. Although the right of free speech and expression is essential to democracy, women and other marginalized groups are frequently silenced by targeted harassment and gendered mobbing on the internet. Victims are frequently compelled to change their public appearances, cancel their accounts, or completely stop participating in public conversation. This limiting impact contradicts the constitutional goal of gender equality enshrined in Articles 14-15[12] by turning internet into an exclusive sphere. In India, the governing bodies are largely subject to the enforcement of constitutional rights under Articles 32 and 226[13]. Nonetheless, private individuals are mostly responsible for DGBV, which is mediated through private social media platforms. In terms of horizontal application, this reality poses important questions. When basic rights are violated on a large scale, the judiciary has increasingly applied constitutional standards to private actors. The state's constitutional obligation to defend its citizens fundamental rights is

[8] The Constitution of India, art. 21
[9] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[10] The Constitution of India, art. 21
[11] The Constitution of India, art. 19(1)(a)
[12] The Constitution of India, arts. 14-15
[13] The Constitution of India, arts. 32 and 226

© 2026 International Journal of Advanced Legal Research

violated when it fails to enact effective protective laws or law enforcement measures for DGBV[14].

II. Legislative Frameworks

The legal mechanism governing the digital violence in India expands multiple statutes, combining specific laws related to technology, codified criminal offences, data protection mandates and administrative guidelines for internet intermediaries.

III.A. The Information Technology Act, 2000[15]

The Act, serves as the main statutory framework for cybercrimes in India. Following 2008 modifications, a number of clauses were included to handle sexual content and privacy violations:

i. Section 66E (Violation of Privacy)[16]: Criminalizes the intentional capturing, publishing or transmitting of images of a person's private areas without their consent, under circumstances violating privacy. The offence carries a punishment of up to three years imprisonment or a fine.

ii. Section 67 (Publishing Obscene Material)[17]: Penalizes the transmission or publication of obscene content in electronic forms.

iii. Section 67A (Publishing Sexually Explicit Content)[18]: Imposes stricter penalties for transmitting or publishing material containing sexually explicit acts in electronic form, punishable by up to five years imprisonment for a first conviction.

iv. Section 66C and Section 66D[19]: Deal with identity theft and cheating by personation using computer resources, which are frequently applied in cases involving fake profiles or impersonation accounts created to harass victims.

III.B. Criminal code framework

[14] Nusrat Ali Rizvi, "The Role of Law in Combatting Gender-Based Violence on Social Media and Online Platforms," 7(1) International Journal for Multidisciplinary Research 1 (2025), https://doi.org/10.36948/ijfmr.2025.v07i01.36813

[15] The Information Technology Act, 2000 (Act 21 of 2000)

[16] The Information Technology Act, 2000 (Act 21 of 2000), s. 66E

[17] The Information Technology Act, 2000 (Act 21 of 2000), s. 67

[18] The Information Technology Act, 2000 (Act 21 of 2000), s. 67A

[19] The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D

© 2026 International Journal of Advanced Legal Research

The IT Act addresses certain technology-specific offenses, but in many instances the conventional provisions of criminal law have been invoked alongside. With the introduction of the Bharatiya Nyaya Sanhita (BNS) 2023[20], several gender-specific offenses have been retained and updated to reflect electronic platforms:

i. Section 78 (Cyberstalking)[21]: Defines stalking to include monitoring a woman's use of the internet, email, or any other form of electronic communication despite her clear indication of disinterest.
ii. Section 77 (Voyeurism)[22]: Criminalizes capturing or disseminating images of a woman engaged in a private act where she would reasonably expect not to be observed.
iii. Sections 74 and 75 (Outraging modesty and sexual harassment)[23]: Applied to electronic communications involving unwelcome sexual advances, requests for sexual favors, or sexually colored remarks.
iv. Sections 351 and 356 (Criminal intimidation and defamation)[24]: Used to prosecute online threats of physical or sexual violence, as well as digital character assassination campaigns.

III.C. Intermediary Guidelines and Data Protection

Because online harms happen on private platforms, regulations place specific obligations on digital intermediaries:

i. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[25]:

   Under Rule 3(1)(b)[26], intermediaries shall exercise due diligence and publish user agreements warning against posting content that is defamatory, obscene, invasive of privacy or gender-insulting. Significantly, Rule 3(2)(b)[27] provides for a fast-track takedown process, upon receipt of a complaint from a victim or an authorized

[20] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
[21] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 78
[22] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 77
[23] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), ss. 74, 75
[24] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), ss. 351, 356
[25] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[26] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(b)
[27] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b)

© 2026 International Journal of Advanced Legal Research

representative, platforms are to take down or disable access to non-consensual explicit or morphed images within 24 hours.

ii. The Digital Personal Data Protection (DPDP) Act, 2023[28]: Provides a legal framework for processing :

It creates a statutory framework for processing of personal data. The Act regulates data fiduciaries and emphasizes consent, but it is primarily concerned with commerce. Its provisions contain sweeping state exemptions and offer limited specific remedies for individual victims of cyber harassment or non-consensual exposure of data.

III. Limitations and statutory lacunae in legal remedies

Despite having these statutory provisions, the existing legal framework has significant deficiencies when confronted with the realities of modern digital violence. The law often struggles to keep up with non-physical harm, new technology platforms and complex online behavior.

IV.A. The challenge with generative AI and synthetic media

One of the most concerning trends in digital gender violence is the rise of deepfakes and generative AI applications. Now, offenders can use one public photograph of a victim to create realistic sexually explicit images or videos of non-consensual nature.

Existing regulations are insufficiently adequate for synthetic media. Section 66E[29], for capturing or publishing the image of a person's actual private area or body. By definition, deepfakes also cover synthetic content that does not involve the direct photography of a physical body without consent.

Likewise, Section 77[30] is based on the premise that the victim was in the act of doing a private ac, in the real world. When an AI model generates explicit images from scratch, however, it creates a statutory hurdle for proving a violation of a given physical space or private act. Prosecutors usually rely on either Section 67A[31], publishing sexually explicit content or general defamation provisions under Section 356[32], but these laws do not address

[28] The Digital Personal Data Protection Act, No. 22 of 2023
[29] The Information Technology Act, 2000 (Act 21 of 2000), s. 66E
[30] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 77
[31] The Information Technology Act, 2000 (Act 21 of 2000), s. 67A
[32] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 356

© 2026 International Journal of Advanced Legal Research

the particular harm of synthetic identity theft. Defamation focuses on reputation rather than bodily dignity, while obscenity laws framed in moral terms shift the focus onto the content itself rather than the violation of the survivor's consent.

IV.B. Coordinated mobbing and doxxing

The act of doxxing, which involves the publication of an individual's private and identifiable information such as their home address, telephone number, place of work, or details of their family contacts, is commonly used to carry out harassment off-line.

There is no specific, codified offence for doxxing under Indian law. When a person's phone number is published online along with abusive material, it is seldom covered by the identity theft provisions (Section 66C)[33], since the individual in question is revealing information rather than taking on the victim's identity. Moreover, unless the doxxing involves clear threats of violence (Section 351)[34] or constitutes sexual harassment (Section 75)[35], police officers usually do not proceed to file a First Information Report (FIR). Also, the existing criminal laws assess each act separately, which makes them inadequate for dealing with coordinated mobbing, in such cases hundreds of users independently make minor derogatory comments that together cause serious psychological harm.

IV.C. Gendered limitations in stalking legislation

Section 78[36] specifically defines cyberstalking as a crime committed by a man against a woman. Although this gender-specific approach takes into account the historical patterns of patriarchal violence, it leads to legal gaps in today's digital environments. Increasingly, cases of digital gender-based violence affect trans, non-binary, and queer people, who therefore do not benefit from the protection offered by Section 78[37]. Moreover, the statutory definition mandates that it must be shown the person accused monitored the victim even though it was clear that the victim had expressed disinterest. In online environments where stalkers use a number of anonymous accounts, automated scraping programmes, or passive surveillance, it would be necessary to prove that the victim had shown disinterest to each and every burner account, thus imposing unreasonable evidential demands.

[33] The Information Technology Act, 2000 (Act 21 of 2000), s. 66C
[34] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 351
[35] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 75
[36] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 78
[37] ibid

© 2026 International Journal of Advanced Legal Research

IV.D. Structural limits of intermediary liability

The 24-hour content removal rule contained in the 2021 Intermediary Rules[38] seems sturdy in theory, but in practice its enforcement is unreliable. Social media companies generally use automated moderation systems which were mainly designed for Western contexts and thus frequently fail to pick up localized Indian languages, regional slangs, or the subtle cultural aspects of abusive behaviour.

Moreover, after an explicit image or deepfake has been uploaded it spreads within minutes over peer-to-peer messaging networks, file-sharing forums, and mirror sites. Taking the original link down from a social media website does not eliminate the content's digital footprint. Since the intermediaries are private organisations, survivors have no direct judicial control with which to enforce the removal of the content from the mirrors without obtaining separate court orders against unknown defendants (John Doe orders)[39], a procedure beyond the reach of most people.

IV. Institutional, Procedural, and Enforcement Barriers

Beyond statutory language, systemic operational obstacles within law enforcement and judicial institutions constitute the limitations of Indian legal protection against DGBV. The effectiveness of a legal remedy depends on the procedural mechanisms used to implement it

V.A. Law enforcement bottlenecks and secondary victimization

The local police station or specialized cybercrime cell is the first point of contact for any victim seeking criminal justice. Systemic gender insensitivity is still a significant obstacle, though.

Law enforcement officials often treat survivors who report digital violence with skepticism, victim-blaming, and moral policing. Police officers frequently counsel women to stop using smartphones, deactivate their social media accounts, or accept that having a digital presence will inevitably result in online abuse. This response deters reporting and trivializes serious constitutional violations.

V.B. Evidentiary complexities

[38] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[39] Sunil Shetty v. Ashok Kumar & Ors., CS(COMM) 234/2024 (Del HC)

© 2026 International Journal of Advanced Legal Research

The procedural requirements for proving digital crimes present significant evidentiary challenges. Under the Bharatiya Sakshya Adhiniyam (BSA) 2023[40], electronic records must be accompanied by specific certificates verifying the authenticity, hash value, and custody chain of the device used to produce the record.

It can be challenging for a regular victim of cyberbullying to gather admissible digital evidence:

i. Preservation of Transient Evidence: In a matter of seconds, the offender or platform algorithms may erase digital content. Defense lawyers frequently contest the admissibility of screenshots unless they are supported by technical metadata, IP log files and device identifiers.
ii. Backlogs in Forensic Laboratories: There are significant operational backlogs in India's state forensic science labs. Forensic extraction of digital devices confiscated during investigations frequently takes months or years, postponing trials and prosecutions.
iii. Cross-Border and Jurisdictional Barriers: The majority of significant digital platforms are based abroad, mostly in the US. Formal Mutual Legal Assistance Treaties (MLATs) or Letters Rogatory must be invoked in order to obtain subscriber identification information, IP logs, or account metadata. These international legal processes take months or years, during which crucial digital evidence is routinely purged by platforms under standard data retention schedules.

V.C. Judicial delays and loss of anonymity in court proceedings

Millions of cases are pending in the Indian legal system. Cybercrime prosecutions proceed slowly through the legal system, requiring victims to make numerous court appearances over long stretches of time.

Importantly, victims are frequently subjected to secondary harm during the legal process itself. Although publishing the identities of victims of specific sexual offenses is forbidden by Section 73[41], this protection is not always applied in cases involving digital harassment. The true names, addresses and specifics of the harassment are frequently published online by court registries, publicly available cause lists, and unredacted judgment summaries. As a

[40] The Bharatiya Sakshya Adhiniyam, No. 47 of 2023
[41] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 73

© 2026 International Journal of Advanced Legal Research

result, victims are caught in a dilemma: seeking legal recourse for online privacy violations necessitates running the risk of additional public exposure in official court documents.

V. Recommendations and the Way Forward

It is necessary to shift from piecemeal statutory amendments to a coherent, survivor-centric body of jurisprudence in order to address the structural issues of digital gender-based violence. While maintaining a foundation in human dignity, operational effectiveness and platform accountability, legal frameworks must adjust to new technological capabilities.

VI.A. Codification of Doxxing and Abuse of Synthetic Media

To specifically address the negative effects of contemporary technology, the legislature must modify statutory provisions:

i. Reformation of the IT Act's Section 66E[42]: The clause should be broadened to include non-consensual creation, generation, alteration, or distribution of artificial intelligence (AI)-manipulated or synthetic intimate images (deepfakes) in addition to physical imagery.

ii. The BNS should include a specific statutory section that defines doxxing as the unlawful publication of a person's personally identifiable information with the intention of causing harassment, violence, or extreme mental distress.

iii. Gender-Inclusive Stalking Laws: In order to provide equal legal protection for transgender, non-binary, and queer individuals who are the targets of digital surveillance and harassment, Section 78[43]should be made gender-neutral with regard to victims.

VI.B. Increasing Technical Redress and Platform Obligations

Beyond mere compliance, social media intermediaries must adhere to higher operational standards:

i. Mandatory Perceptual Hashing: For reported non-consensual intimate imagery, platforms operating in India ought to be mandated by law to use proactive perceptual

[42] The Information Technology Act, 2000 (Act 21 of 2000), s. 66E
[43] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), s. 78

© 2026 International Journal of Advanced Legal Research

hashing technology (like PhotoDNA). To stop re-uploads, the platform should block the distinct digital signature of any explicit image or deepfake that has been reported and eliminated.

ii. Algorithmic Transparency and Localized Moderation: In order to ensure that moderation models comprehend gendered slurs, abusive metaphors, and localized slang, intermediaries must invest in content moderation capabilities in Indian regional languages.

VI.C. Modernization of Institutions and Support for Survivors

To avoid secondary trauma, judicial systems and enforcement agencies need to be updated:

i. Specialized Fast-Track Cyber Courts: To handle DGBV complaints within a set statutory timeframe, district-level special courts with digital evidence infrastructure should be established.

ii. Automated Anonymization of Court Records: Mandatory digital protocols should be put in place by the judiciary to automatically remove survivors' personal information, account handles, and private evidence from public cause lists, court orders, and online court archives.

iii. Comprehensive Sensitivity Training: Training on digital forensics, trauma-informed interviewing, and the constitutional aspects of digital privacy is required for both police officers and attorneys.

VI. Conclusion

Digital gender-based violence represents a fundamental challenge to the constitutional vision of an egalitarian society. The transformation of digital networks into venues for gendered harassment, non-consensual synthetic exploitation, and surveillance threatens the rights to privacy, personal autonomy, and human dignity guaranteed under Article 21[44]

As this analysis demonstrates, India's legal infrastructure remains fragmented. The existing statutory framework offer partial protections, but they are consistently undermined by statutory lacunae surrounding emerging technologies like generative AI, strict physical

[44] The Constitution of India, art. 21

© 2026 International Journal of Advanced Legal Research

evidence definitions, and inadequate provisions for doxxing. These legislative gaps are compounded by systemic enforcement failures, forensic backlogs and institutional insensitivity within law enforcement agencies.

To bridge the gap between constitutional principles and daily digital realities, the state must modernize its cyber jurisprudence. This requires clear statutory recognition of synthetic digital harms, stricter algorithmic accountability for social media platforms, and specialized, survivor-centric judicial procedures. Only by centering human dignity and fundamental rights can the law ensure that cyberspace remains an inclusive, secure, and democratic environment for all citizens.

© 2026 International Journal of Advanced Legal Research