

Online Violence against Women in Cyberspace: Judicial Rperspective

Dr Renu Saini

ABSTRACT

Violence against women exists in many forms and in all areas of society. With recent technological advancement and digital literacy policies have brought social media age, institutional challenges continue to persist, gender equality remaining one of the largest issues. Women in India continue to experience victimisation of online violence and it continues to remain majorly unreported due to patriarchal structures, fear of family rejection and inequality in offline society structure.¹ Moreover, women who are public figures, belong to a particular group or work for social cause such as human rights activists, women politicians, bloggers, women influencers, journalists, women from minorities, lesbian, transgender women and women with disabilities are particularly targeted by online violence.²

In 1993, United Nations Declaration on the Elimination of Violence against Women defines “Violence as any act that results in, or is likely to result in, physical, sexual, or psychological harm or suffering to women, including threats of such acts, coercion, or arbitrary deprivation of liberty, whether occurring in public or private life.”³ When discussing “online violence against women” a question which is often asked is “Is it actually violence?”, though many international documents and conventions have long back recognized psychological and emotional abuse as a form of violence, including many forms of abuse which are facilitated by technology. While there is still a lack of comprehensive global definition and data on online and technology facilitated violence, research suggests that women are both disproportionately targeted and suffer serious consequences as a result. When women and girls do have access to the internet, they face online violence more often than men, through a continuum of multiple, recurring and interrelated forms of gender-based violence.⁴

In current times, online harassment has impacted the majority of women who use online space to socialise, earn a living and expressing their opinions. To some extent it interferes with their personal and professional relationships. It further makes them vulnerable to online and offline sexual violence and brands them as inferior sexual objects. For the longest time, no matter how grave and serious harm cybercrimes cause to women and their lives, the public and society always tends to ignore and trivialise it. Ignoring the trolls and abuse, limiting sharing personal information or going offline are some suggested ways to deal with violence happening in cyberspace against women. These suggestive measures to protect women from technology facilitated abuse and online violence is based on the problematic assumption that cybercrimes happen to certain online behaviours and share on the internet. It is very important to understand how abuse to create safe cyberspace for women and girls and whose responsibility it is to prevent and curb online abuse and harassment. Without an improved system of providing protection and prevention online violence faced by women and girls will continue to remain a challenge to their safety.

Judicial response has thus emerged as a central mechanism in regulating online violence against women. While legislative frameworks provide the structural basis for addressing cyber offences, it is the judiciary that interprets statutory provisions, delineates constitutional protections, and balances competing rights in the digital domain. Courts are increasingly required to reconcile freedom of speech with dignity and privacy, and technological advancement with constitutional accountability. The resulting jurisprudence reflects an evolving constitutional discourse that seeks to adapt traditional legal principles to the realities of the digital age.⁵ The architecture of cyberspace facilitates the replication and amplification of abusive content in ways that are difficult to control or reverse. A single act of uploading or sharing intimate material without consent can result in continuous circulation across multiple platforms, causing enduring psychological trauma, reputational harm, and social exclusion. The persistence of digital records further compounds the injury, as victims are often unable to fully erase the offending content from the internet. This permanence creates a condition of ongoing victimisation, where harm is not confined to a single incident but is

¹*Assistant Professor , Khalsa College Of Law , Amritsar-143001

PriyaKumari and Anatoly Gruz, “Mapping out Violence Against Women of Influence on Twitter Using the Cyber-Lifestyle Routine Activity Theory” 65(5) Sage Publishing 69 (2021).

²Ibid.

³UN General Assembly, Declaration on the Elimination of Violence Against Women, GA Res 48/104, GAOR, UN DOC Article 1 (Dec. 20, 1993).

⁴ReemAlsalem, United Nations Special Rapporteur on Violence Against Women, its Causes and Consequences, UNHR Doc A/HRC/47/26 (April 19, 2021)

⁵PavanDuggal, Cyberlaw: The Indian Perspective 210 (Saakshar Law Publications, New Delhi, 2021).

continuously reproduced over time. Consequently, online violence against women must be understood not merely as an extension of offline abuse, but as a qualitatively distinct phenomenon that demands specialised legal and constitutional responses.

A significant feature of contemporary Indian constitutional adjudication is the movement from a purely negative conception of rights towards recognition of positive obligations of the State. Scholars have observed that digital rights cannot be protected merely by restraining state interference; effective protection also requires institutional mechanisms capable of preventing, investigating, and remedying technology-facilitated harm. In the context of women's rights, this shift is particularly important because online violence often produces chilling effects on participation in education, employment, political discourse, and social life.⁶

The constitutional vocabulary used by Indian courts in cyber-related cases is drawn primarily from Articles 14, 15, 19, and 21, but the judicial emphasis has increasingly fallen on dignity, privacy, and equality. Privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v Union of India provided a constitutional foundation for addressing many forms of digital abuse that involve unauthorised access, dissemination, or manipulation of personal information. However, privacy is not the sole constitutional value at stake; online violence against women also implicates reputation, bodily integrity, decisional autonomy, and equal participation in public spaces. The rapid expansion of the internet has turned digital spaces into vital hubs for modern human engagement, yet it has simultaneously accelerated a dangerous trend: technology – facilitated, gender – based cyber violence. In cyberspace, perpetrators easily abuse digital tools to deploy targeted harassment, non – consensual dissemination of private images, and deepfakes while hiding behind a veil of anonymity.

This form of digital hostility acts as an electronic continuation of historical structural misogyny, engineered specifically to intimidate and drive women out of public online discourse. Because digital spaces are now inseparable from everyday realities, the legal ecosystem must rapidly adapt. This rise is closely linked to the growing penetration of internet services, increased use of smartphones, and expanding participation of women in digital platforms. The digital environment, therefore, presents a paradox: it is both an instrument of empowerment and a site of intensified gendered harm. Rather than adhering blindly to outdated, physical – world legal standards, courts are being called upon to dynamically reinterpret existing laws. This chapter does not repeat the legislative framework discussed in the previous chapter. Instead, it critically examines how Indian courts have responded to technology-facilitated violence against women through constitutional interpretation and judicial innovation. The analysis focuses on the evolution of judicial reasoning, the treatment of privacy and dignity in digital contexts, the constitutional limits of online speech, the responsibility of intermediaries, and the effectiveness of judicial remedies. It also engages with contemporary scholarly literature and recent legal developments to evaluate whether the existing judicial approach is adequate to address the structural and technological dimensions of online violence against women. Thus judiciary acts as a primary guardian, holding the unique responsibility of defining the boundary between constitutional speech and a woman's fundamental right to privacy, personal dignity and public safety.

Evolution of Judicial Approach to Cyber Violence against Women

The judicial response to cyber violence against women in India has evolved through distinct phases reflecting broader transformations in constitutional jurisprudence, technological development, and societal understanding of gender-based harm. In the early years of internet regulation, courts primarily approached cyber offences through the lens of technical illegality and criminal procedure. Judicial attention was largely directed towards questions of jurisdiction, admissibility of electronic evidence, and the applicability of existing penal provisions to online conduct. Gendered harms occurring in digital spaces were often treated as extensions of conventional offences rather than as a distinct form of structural violence requiring specialised constitutional analysis.⁷

This initial approach was influenced by the limited scope of the Information Technology Act, 2000 in its original form. The statute was enacted primarily to facilitate electronic commerce and recognise digital records and signatures, while issues such as cyberstalking, image-based abuse, and platform-enabled harassment received comparatively little legislative attention. Consequently, courts frequently relied on provisions of the Indian Penal Code dealing with obscenity, criminal intimidation, defamation, insult to modesty, and harassment to address online misconduct directed against women. Scholars have noted that this reliance produced a fragmented jurisprudence because digital harms were forced into categories designed for pre-internet contexts.⁸

A gradual shift became visible after the 2008 amendments to the Information Technology Act, which introduced provisions relating to sexually explicit material, privacy violations, identity theft, and cyber terrorism. Although these amendments did not create a comprehensive framework for technology-facilitated gender violence, they signalled

⁶Aparna Viswanath, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* 325 (LexisNexis, New Delhi, 2nd edn., 2012).

⁷Yatindra Singh, *Cyber Laws* 145 (Universal Law Publishing Co. Pvt. Ltd., New Delhi, 5th edn., 2016).

⁸Indian Penal Code, 1860, ss. 354A, 354D, 499, 503, 509, BNS. Ss. 75, 78, 356(1), 351(1), 79.

legislative recognition that digital spaces could generate distinct forms of harm. Judicial decisions thereafter began to engage more directly with the privacy and dignity implications of online conduct, particularly in cases involving unauthorised dissemination of personal images and electronic harassment.⁹

The second phase of judicial evolution was marked by the increasing influence of transformative constitutionalism. The Supreme Court's post-Maneka Gandhi jurisprudence had already expanded Article 21 beyond physical liberty, but the application of this expansive approach to digital environments gained momentum only in the last decade. Courts started recognising that online abuse could interfere with an individual's autonomy, reputation, mental well-being, and ability to participate in public life. This development was especially significant for women, who are disproportionately targeted through sexualised abuse, threats of violence, coordinated trolling, and non-consensual image circulation.¹⁰

The decision in Justice K.S. Puttaswamy (Retd.) v Union of India represents a constitutional turning point in this evolution. By recognising informational privacy as a fundamental right, the Supreme Court provided a doctrinal foundation for understanding many forms of cyber violence as violations of constitutional rights rather than merely statutory offences. The judgment acknowledged that control over personal information is integral to dignity and autonomy, thereby directly influencing judicial reasoning in subsequent cases involving digital identity, intimate content, and online surveillance. Commentators have observed that Puttaswamy transformed the constitutional conversation from "privacy versus regulation" to "privacy as a precondition for equal citizenship in the digital age."¹¹

Another important stage in judicial development concerns the relationship between free speech and online harm. In ShreyaSinghal v Union of India, the Supreme Court invalidated Section 66A of the Information Technology Act on grounds of vagueness and overbreadth. While the judgment strongly protected legitimate online expression, it did not create immunity for abusive or criminal conduct. The Court carefully distinguished constitutionally protected speech from speech that may be regulated under Article 19(2), including obscenity, defamation, incitement, and criminal intimidation. This distinction remains central to contemporary disputes involving online harassment of women because perpetrators often invoke free speech to resist accountability.¹²

The evolution of judicial approach has also been shaped by growing awareness of the chilling effect of online violence. Courts have increasingly acknowledged that persistent harassment, threats, and coordinated abuse can force women to withdraw from digital platforms, restrict professional opportunities, and discourage participation in political or social discourse. This understanding aligns with international scholarship, particularly the work of Danielle Keats Citron, who argues that cyber harassment undermines democratic participation by disproportionately silencing women and other vulnerable groups. Indian courts have not always explicitly cited this scholarship, but recent judicial reasoning reflects a similar concern with the exclusionary consequences of digital abuse.¹³

High Courts have contributed significantly to this evolution by adopting victim-centric approaches in cases involving fake social media profiles, morphed images, revenge pornography, and cyberstalking. These decisions increasingly emphasise prompt removal of harmful content, protection of victim identity, and effective investigation. Although doctrinal consistency is still developing, the cumulative effect of these judgments has been to shift the focus from purely punitive responses towards protection of dignity and prevention of continuing harm.¹⁴

Despite these advances, important limitations remain. Judicial responses are often reactive rather than preventive, and courts continue to depend on statutory provisions that were not specifically designed to address the scale and complexity of contemporary platform-mediated abuse. Delays in investigation, jurisdictional difficulties, inconsistent intermediary cooperation, and limited digital forensic capacity frequently weaken the effectiveness of judicial remedies. Moreover, scholars have criticised the absence of a coherent doctrinal framework specifically addressing technology-facilitated gender-based violence, arguing that courts still oscillate between criminal law, privacy law, and constitutional law without fully integrating these perspectives.¹⁵

The evolution of Indian judicial approach to cyber violence against women therefore reflects a movement from technical regulation to rights-based constitutional protection, but the transition remains incomplete. Courts have progressively incorporated the values of dignity, privacy, autonomy, and equal participation into digital rights

⁹PavanDuggal, *Cyberlaw: The Indian Perspective* 245 (Saakshar Law Publications, New Delhi, 2021).

¹⁰ V.N. Shukla, *Constitution of India* 412 (Eastern Book Company, Lucknow, 13th edn., 2017).

¹¹ Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.

¹² ShreyaSinghal v Union of India (2015) 5 SCC 1.

¹³ X v State of Maharashtra, 2021 SCC OnLineBom 458, para 38.

¹⁴ MrinalSatish and Aparna Chandra, "Technology-Facilitated Gender Violence and the Limits of Indian Criminal Law" (2024) 15 Indian Law Review 221, 236–242.

¹⁵ Crime in India 2024, Chapter XIV (Ministry of Home Affairs, Government of India, 2025).

jurisprudence, yet the challenge of developing a consistent and comprehensive constitutional response to technology-facilitated gender violence continues to confront the Indian legal system.

Privacy, Dignity and Informational Autonomy in Digital Spaces

The constitutional protection against online violence against women is increasingly anchored in the interrelated concepts of privacy, dignity, and informational autonomy. Digital technologies have fundamentally altered the relationship between individuals and personal information by enabling continuous collection, storage, reproduction, and dissemination of data across multiple platforms. For women, this transformation has generated new vulnerabilities, including cyberstalking, doxing, impersonation, non-consensual sharing of intimate images, and algorithmically amplified harassment. Judicial interpretation has therefore moved beyond the traditional understanding of privacy as secrecy and has begun to treat control over personal information as an essential condition for autonomy and equal participation in society.¹⁶

The most significant constitutional development in this context is the decision of the nine-judge Bench of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v Union of India*. The Court held that privacy is a constitutionally protected right deriving from the guarantees of life, personal liberty, dignity, and freedom under Part III of the Constitution. Importantly, the judgment identified informational privacy as a distinct dimension of the right, recognising that individuals must have the ability to determine how personal information is collected, used, and disseminated. This reasoning is directly relevant to online violence against women because many forms of digital abuse involve the loss of control over intimate or identity-related information.¹⁷

Scholarly commentary has emphasised that informational privacy is not merely a matter of confidentiality but a question of power and agency. Danielle Citron argues that the unauthorized circulation of intimate content deprives individuals of control over their social identity and exposes them to long-term reputational and psychological harm. Similarly, Ronald Krotoszynski describes privacy as a precondition for meaningful autonomy in networked societies, where personal information can be replicated and redistributed indefinitely. These insights help explain why image-based abuse and digital impersonation cannot be treated as minor offences; they strike at the victim's ability to shape her own identity and social relationships.¹⁸

Indian courts have increasingly reflected this understanding in cases involving intimate images and digital identity. In *State of West Bengal v AnimeshBoxi*, the Calcutta High Court treated the non-consensual circulation of intimate images as a grave violation of the victim's privacy and dignity, emphasizing that the harm extends beyond the initial act of disclosure because digital content can continue to circulate indefinitely. The court also recognized the severe psychological and social consequences of such conduct, thereby moving the analysis beyond obscenity towards a rights-based framework centered on autonomy and dignity.¹⁹

The constitutional idea of dignity has played an equally important role in judicial reasoning. Indian constitutional jurisprudence has consistently interpreted dignity as an inseparable component of Article 21. In digital contexts, dignity is implicated when women are subjected to sexualized abuse, morphed images, deepfake pornography, coordinated trolling, or public shaming. Such acts reduce the individual to an object of humiliation and undermine her status as an equal participant in society. Courts have therefore increasingly viewed online abuse as an assault on constitutional personhood rather than merely a violation of reputation.²⁰

The relationship between privacy and dignity is particularly visible in cases involving non-consensual intimate image distribution. Unlike traditional obscenity offences, these cases do not primarily concern public morality; they concern the absence of consent and the resulting loss of control over one's body and identity. Comparative scholarship has influenced Indian legal discourse by emphasizing that the core wrong lies in the betrayal of trust and the deprivation of sexual and informational autonomy. Recent academic work in Indian constitutional law similarly argues that consent should be the central organizing principle for understanding image-based abuse in digital environments.²¹

Technological developments such as deepfake technology and artificial intelligence-generated sexual content have significantly complicated constitutional analysis in the context of online violence against women. These technologies

¹⁶Constitution of India, arts 14, 19 and 21; National Crime Records Bureau, *Crime in India 2024* (Ministry of Home Affairs 2025), chapter 14.

¹⁷Aparna Chandra, "Consent, Privacy and Digital Sexual Violence" (2025) 17 *NUJS Law Review* 112, 120–129.

¹⁸*Ibid.*

¹⁹*State of West Bengal v AnimeshBoxi*, 2018 SCC OnLine Cal 3182. See also M.P. Jain, *Indian Constitutional Law* 1350 (LexisNexis, New Delhi, 8th edn, 2018).

²⁰Aparna Chandra, "Consent, Privacy and Digital Sexual Violence" (2025) 17 *NUJS Law Review* 112, 125.

²¹MrinalSatish and Aparna Chandra, "Technology-Facilitated Gender Violence and the Limits of Indian Criminal Law" (2024) 15 *Indian Law Review* 221, 238–240.

enable the creation of highly realistic yet fabricated intimate images and videos, often without the consent or even knowledge of the victim. Such content causes severe reputational, psychological, and social harm, even in cases where no original image exists. Indian legal scholarship has increasingly recognised such practices as a form of technologically mediated sexual exploitation that undermines personal autonomy and dignity. Although Indian jurisprudence on deepfakes is still evolving, the principles of informational privacy, dignity, and autonomy articulated by the Supreme Court provide a constitutional basis for addressing such harms.²²

Privacy in digital spaces also has a collective and democratic dimension. Empirical studies indicate that women who experience severe online harassment often withdraw from social media, reduce public engagement, or avoid expressing controversial opinions. The loss of privacy therefore affects not only individual autonomy but also the inclusiveness of democratic discourse. Constitutional protection of informational autonomy consequently serves a broader purpose: it helps ensure that women can participate in digital public spheres without disproportionate fear of surveillance, exposure, or humiliation.²³

Despite these doctrinal advances, significant gaps remain in the judicial protection of informational autonomy. Indian courts have not yet developed a fully coherent framework for balancing privacy with freedom of expression, journalistic interests, platform governance, and technological innovation. Remedies are often fragmented, with victims required to pursue multiple proceedings for content removal, criminal prosecution, and compensation. Moreover, the absence of comprehensive data protection legislation for much of the relevant period has limited the effectiveness of privacy-based claims in cases involving private actors and digital platforms.²⁴

Nevertheless, the trajectory of constitutional jurisprudence is clear. Indian courts are gradually reconceptualising privacy from a narrow right “to be let alone” into a broader guarantee of control over personal information, bodily representation, and digital identity. For women facing technology-facilitated violence, this shift is of profound significance because it recognises that equality and dignity in the digital age depend upon the preservation of informational autonomy.

Freedom of Expression and Constitutional Limits on Online Abuse

The constitutional regulation of online abuse requires courts to navigate one of the most difficult tensions in democratic societies: the relationship between freedom of expression and protection from harm. Digital platforms have become central spaces for political participation, social interaction, journalism, activism, and cultural expression. Any legal response to online violence against women must therefore avoid creating a framework that suppresses legitimate speech or enables excessive state control over the internet. At the same time, constitutional protection of expression cannot be interpreted as a licence for harassment, intimidation, sexual abuse, or coordinated attacks designed to silence women. The judicial challenge lies in distinguishing between protected expression and conduct that infringes the constitutional rights of others.²⁵

Article 19(1)(a) of the Constitution guarantees freedom of speech and expression, which has been consistently recognised as a foundational value of constitutional democracy. In the digital age, this right has assumed greater significance due to the expanded reach of internet-based communication. Women have increasingly utilised digital platforms for political mobilisation, professional advancement, and social advocacy. Consequently, restrictions on online speech must be carefully calibrated so as not to disproportionately limit women’s participation in public discourse.²⁶

However, the constitutional guarantee is subject to the reasonable restrictions enumerated in Article 19(2), including defamation, public order, decency, morality, incitement to an offence, and other specified grounds. The key constitutional question is not whether online speech may ever be regulated, but how regulation can be structured so that it targets harmful conduct without chilling legitimate expression. This distinction is particularly important in cases involving misogynistic abuse, threats of sexual violence, doxxing, deepfake pornography, and coordinated trolling campaigns. Such conduct often combines expressive elements with intentional harm, making the boundary between speech and abuse constitutionally significant.²⁷

²²Ministry of Women and Child Development, Report on Cyber Crimes against Women and Children 52 (Government of India, 2023).

²³*Secretary, Ministry of Information and Broadcasting v Cricket Association of Bengal*, (1995) 2 SCC 161.

²⁴Digital Personal Data Protection Act 2023; Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) 45–52.

²⁵Constitution of India, art 19(1)(a).

²⁶Ministry of Women and Child Development, Report on Cyber Crimes against Women and Children 52 (Government of India, 2023).

²⁷Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 45–52 (Government of India, 2018).

The Supreme Court's decision in *ShreyaSinghal v Union of India* remains the leading authority on online speech regulation in India. The Court struck down Section 66A of the Information Technology Act, 2000 on the ground that its vague and overbroad language created an unacceptable chilling effect on free expression. Importantly, the judgment did not hold that harmful online speech is immune from regulation. Rather, it clarified that restrictions must be grounded in the specific categories recognized under Article 19(2) and must satisfy constitutional standards of clarity and proportionality. The Court distinguished between mere discussion or advocacy, which is protected, and speech that reaches the level of incitement or other constitutionally regulable forms.²⁸

From the perspective of online violence against women, *ShreyaSinghal* has a dual significance. On one hand, it protects women's own freedom to speak, criticize, organize, and participate in digital public life without fear of arbitrary censorship. On the other hand, it prevents the use of vague criminal provisions that could be selectively enforced against distinguish or marginalized voices. Scholars have noted that overly broad cyber laws often end up harming the very groups they are purportedly designed to protect. A rights-based approach therefore requires precision in defining unlawful online conduct.²⁹

At the same time, feminist legal scholarship has cautioned against treating all online abuse as protected expression. Danielle Citron argues that severe cyber harassment functions less as participation in public debate and more as a mechanism of exclusion that drives women out of digital spaces. Similarly, Indian scholars have emphasized that coordinated misogynistic abuse can undermine substantive equality by imposing disproportionate burdens on women's participation in public discourse. These arguments support a constitutional approach that recognises the silencing effect of targeted online abuse rather than viewing it solely through the lens of speaker autonomy.³⁰

Indian courts have increasingly acknowledged this concern in cases involving threats, harassment, and non-consensual sexual content. Judicial reasoning has begun to emphasize that freedom of expression does not protect speech that violates privacy, dignity, reputation, or bodily autonomy. In several cases, courts have directed the removal of harmful content and protected the identity of victims, particularly where continued circulation of material would perpetuate the violation. Although the doctrinal foundations of these orders vary, the underlying principle is that constitutional rights must be balanced in a manner that preserves the equal citizenship of women in digital spaces.³¹

A further complexity arises from the role of intermediaries and platform governance. Decisions about content removal are increasingly made not only by courts and governments but also by private technology companies applying their own community standards. This raises concerns about transparency, due process, and accountability. Excessive deference to platforms may leave victims without effective remedies, while excessive state control may threaten free expression. Contemporary constitutional scholarship therefore advocates a model of co-regulatory accountability, in which platforms bear responsibilities to address clearly unlawful and harmful content while procedural safeguards protect legitimate speech.³²

The legislative foundation for addressing cyberstalking is found primarily in Section 354D of the Indian Penal Code, 1860, which criminalized stalking, including monitoring a woman's use of electronic communication. The provision was introduced after the recommendations that followed the Justice Verma Committee Report, which emphasized the need to address emerging forms of gender-based violence facilitated by technology. Although the statutory recognition was significant, judicial interpretation has been necessary to determine the scope of electronic monitoring, repeated online contact, and the evidentiary standards applicable to digital harassment.³³

Courts have generally adopted a victim-centric understanding of cyberstalking by focusing on the impact of the conduct rather than requiring proof of physical proximity or direct confrontation. In several cases, High Courts have treated repeated messaging, creation of fake accounts, circulation of personal photograph, and persistent online surveillance as sufficient to attract criminal liability. Judicial reasoning increasingly acknowledges that digital technologies enable continuous intrusion into the victim's life, making harassment possible regardless of geographical distance. This

²⁸ *ShreyaSinghal v Union of India* (2015) 5 SCC 1.

²⁹ *Secretary, Ministry of Information and Broadcasting v Cricket Association of Bengal*, (1995) 2 SCC 161.

³⁰ Constitution of India, art 19(2); MadhaviGoradia Divan, *Facets of Media Law* 201–209 (Eastern Book Company, Lucknow, 2nd edn, 2013).

³¹ *State of West Bengal v AnimeshBoxi*, 2018 SCC OnLine Cal 3182.

³² MrinalSatish and Aparna Chandra, "Technology-Facilitated Gender Violence" (2024) 15 *Indian Law Review* 221, 233.

³³ Justice J.S. Verma Committee, Report of the Committee on Amendments to Criminal Law p. 244 (Government of India, 2013).

recognition is particularly important for women who may face abuse from former partners, acquaintances, colleagues, or anonymous individuals.³⁴

The Bombay High Court in *X v State of Maharashtra* emphasized the seriousness of online harassment involving fake social media profiles and unauthorized use of personal images. The court recognized that such conduct can cause severe emotional distress and reputational harm, especially when the material is disseminated to a wide audience. Importantly, the decision highlighted the need for prompt investigative action and protection of the victim's identity, reflecting a broader judicial concern with preventing the continuation of harm rather than merely punishing past conduct.³⁵

Judicial responses have also been influenced by the understanding that cyberstalking often involves patterns of coercive control. Feminist scholars have argued that digital surveillance can become a mechanism for maintaining power over women, particularly in intimate or former intimate relationships. Continuous monitoring of social media activity, location sharing, online interactions, and communication records may create an environment of fear and dependency. Although Indian courts have not always used the language of coercive control explicitly, recent decisions increasingly consider the broader context of repeated and targeted conduct rather than evaluating each act in isolation.³⁶

A recurring challenge in cyberstalking cases is the issue of electronic evidence. Screenshots, chat logs, metadata, IP addresses, and platform records are often crucial for establishing repeated conduct and identifying the perpetrator. The Supreme Court's jurisprudence on electronic evidence, particularly regarding the admissibility of electronic records, has therefore become indirectly relevant to the prosecution of online harassment. Courts have emphasized the importance of proper collection, preservation, and certification of digital evidence, although practical difficulties continue to affect effective enforcement.³⁷

Another significant aspect of judicial response concerns the psychological harm caused by online harassment. Traditional criminal law has often prioritized physical injury, but courts are increasingly acknowledging that persistent digital abuse can produce anxiety, depression, fear, sleep disturbance, and social withdrawal. Empirical studies indicate that women subjected to severe online harassment frequently restrict their online presence, avoid professional networking, or disengage from public debate. Judicial recognition of these consequences strengthens the constitutional linkage between cyberstalking and the rights to dignity, privacy, and meaningful participation in social life.³⁸

Despite these developments, enforcement remains inconsistent. Police authorities may sometimes treat online harassment as trivial, advise victims to block the perpetrator, or fail to appreciate the cumulative nature of repeated digital abuse. Scholars have criticized this tendency as reflecting a gap between formal criminalization and substantive protection. Delays in obtaining data from intermediaries, lack of specialized cyber training, and limited digital forensic resources further weaken the effectiveness of judicial remedies. Courts have occasionally expressed concern about these institutional deficiencies, but systemic implementation remains uneven across jurisdictions.³⁹

The transition from the Indian Penal Code to the Bharatiya Nyaya Sanhita, 2023 has retained the offence of stalking, including electronic monitoring, indicating legislative continuity in recognizing technology-facilitated stalking as a serious offence. However, the effectiveness of the new framework will depend largely on judicial interpretation, investigative capacity, and the willingness of courts to continue adopting a rights-based and gender-sensitive approach. The core challenge is not merely the existence of a penal provision but the development of a coherent jurisprudence that understands cyberstalking as a violation of autonomy, privacy, dignity, and equal participation in digital spaces.⁴⁰ Indian judicial responses to cyberstalking and online harassment therefore reveal an important doctrinal shift. Courts are gradually moving away from viewing online abuse as isolated offensive communication and toward recognizing it as a pattern of targeted conduct capable of undermining constitutional values. While significant gaps remain in enforcement and institutional capacity, the emerging jurisprudence provides an increasingly robust foundation for protecting women against persistent digital harassment and surveillance.

³⁴ Aparna Viswanath, *Cyber Law: Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cyber Crimes* p. 259 (LexisNexis, New Delhi, 2012).

³⁵ *State of Maharashtra*, 2021 SCC OnLine Bom 458, para 21.

³⁶ Mrinal Satish and Aparna Chandra, "Technology-Facilitated Gender Violence and the Limits of Indian Criminal Law" (2024) 15 *Indian Law Review* 221, 229.

³⁷ *Arjun Pradeep Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1, para 65.

³⁸ National Commission for Women, *Report on Cyber Crime against Women* p. 67 (NCW, New Delhi, 2022).

³⁹ Mrinal Satish and Aparna Chandra, "Technology-Facilitated Gender Violence" (2024) 15 *Indian Law Review* 221, 236.

⁴⁰ Bharatiya Nyaya Sanhita 2023, s 78 (stalking); Ministry of Home Affairs, *Comparative Table: IPC and BNS Provisions* (2024).

Judicial Response to Non-Consensual Intimate Image Distribution and Image-Based Abuse

The non-consensual distribution of intimate images has emerged as one of the most serious forms of online violence against women. Commonly described as image-based sexual abuse, the phenomenon includes the sharing of private photographs or videos without consent, threats to publish intimate material, circulation of morphed or fabricated sexual images, and the dissemination of content obtained through relationships of trust. The harm caused by such conduct is not limited to embarrassment or reputational injury; it affects bodily autonomy, sexual privacy, psychological integrity, and social participation. Because digital content can be copied, stored, and redistributed indefinitely, the violation often becomes continuous rather than momentary. Indian courts have increasingly recognized that these offences require a constitutional analysis centered on consent, dignity, and informational control rather than merely on obscenity or morality.⁴¹

For many years, prosecutions involving intimate images were pursued through a combination of provisions relating to obscenity under the Indian Penal Code and Sections 67 and 67A of the Information Technology Act, 2000. This framework was conceptually inadequate because it focused on the nature of the content rather than on the absence of consent. Feminist legal scholars have criticized obscenity-based approaches for shifting attention away from the victim's autonomy and toward public morality. Contemporary scholarship argues that the central wrong in image-based abuse is the unauthorized exercise of power over another person's sexual identity and digital representation.⁴²

A significant judicial development occurred in *State of West Bengal v AnimeshBoxi*, where the Calcutta High Court treated the non-consensual circulation of intimate images as a grave violation of privacy and dignity. The court emphasized that the victim had not consented to the dissemination of the images and acknowledged the severe psychological and social consequences of digital circulation. Importantly, the decision moved beyond a narrow obscenity analysis and recognized the continuing nature of the harm caused by online dissemination. The judgment is widely regarded as one of the earliest Indian decisions to articulate a rights-based understanding of image-based abuse.⁴³

The constitutional foundation for this approach was strengthened by *Justice K.S. Puttaswamy (Retd.) v Union of India*, which recognized informational privacy and decisional autonomy as components of Article 21. Applied to intimate images, the judgment implies that individuals possess a constitutional interest in controlling the disclosure and use of representations of their bodies and private lives. The unauthorized publication of such material therefore implicates not only statutory offences but also constitutional guarantees of dignity, autonomy, and personal liberty. Scholars have observed that Puttaswamy enables Indian courts to conceptualize image-based abuse as a violation of sexual and informational self-determination.⁴⁴

Judicial responses have also begun to address the problem of morphed and fabricated images. Digital editing tools and artificial intelligence systems can create highly realistic sexual content depicting a person who never participated in the creation of such material. These technologies intensify the harm because they undermine trust in visual evidence and expose victims to humiliation even in the absence of any original intimate photograph. While Indian jurisprudence on deepfake pornography is still developing, courts have increasingly recognized that fabricated sexual images can be as damaging as authentic ones because the injury lies in the false attribution and public association of the victim with the content.⁴⁵

Another important aspect of judicial response concerns threats to disclose intimate material, often referred to as sextortion or image-based blackmail. In many cases, the threat itself is used to coerce continued relationships, sexual acts, financial payments, or silence. Courts have treated such conduct as involving criminal intimidation, extortion, and violations of privacy. The constitutional significance of these cases lies in the recognition that coercive control exercised through digital material can severely impair personal autonomy and freedom of choice.⁴⁶

Victim protection has become a recurring concern in judicial proceedings. Courts have increasingly directed that the identity of victims be protected, that harmful content be removed expeditiously, and that investigative agencies act promptly to prevent further circulation. However, practical difficulties remain substantial. Content may be mirrored across multiple platforms, shared through encrypted services, stored on foreign servers, or reposted by third parties. As

⁴¹National Crime Records Bureau, *Crime in India 2024*ch. XIV, p. 318 (Ministry of Home Affairs, New Delhi, 2025).

⁴²Information Technology Act 2000, ss 67 and 67A.

⁴³*State of West Bengal v AnimeshBoxi*, 2018 SCC OnLine Cal 3182.

⁴⁴*Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1, para 297.

⁴⁵Ministry of Electronics and Information Technology, *Advisory on Deepfake and AI Generated Content* p. 4 (Government of India, 2024).

⁴⁶Indian Penal Code 1860, s. 503 (criminal intimidation), BNS s. 351(1)

a result, removal orders do not always provide complete relief, and victims may continue to experience recurring exposure and harassment.⁴⁷

Comparative scholarship has influenced Indian academic debate by emphasizing that image-based abuse should be understood as a form of sexual violence rather than a property or obscenity offence. Clare McGlynn and Erika Rackley argue that the harm arises from the violation of sexual autonomy and the exploitation of gendered power structures. Indian scholars have increasingly adopted this perspective, contending that constitutional jurisprudence should place consent at the center of legal analysis. This approach aligns with the broader trajectory of Indian constitutional law, which has progressively emphasized dignity, autonomy, and equality in matters involving body and sexual integrity.⁴⁸

Despite doctrinal progress, significant gaps persist. The current legal framework remains fragmented across provisions relating to obscenity, privacy, intimidation, extortion, and harassment. There is no dedicated comprehensive legislation addressing image-based sexual abuse in all its forms, particularly AI-generated content and repeated redistribution by multiple actors. Judicial remedies are also often reactive, becoming available only after substantial harm has already occurred. Scholars have therefore called for a more integrated framework combining criminal sanctions, rapid content removal, victim compensation, psychological support, and platform accountability.⁴⁹

The emerging judicial approach nevertheless represents a substantial transformation in Indian law. Courts are gradually moving from a morality-based understanding of intimate images toward a constitutional framework grounded in consent, dignity, privacy, and autonomy. This shift is especially important for women because it recognizes that control over one's body and digital representation is an essential component of equal citizenship in the digital age. The future development of Indian jurisprudence on deepfakes, AI-generated sexual content, and cross-platform dissemination will determine how effectively these constitutional principles can respond to rapidly evolving forms of image-based abuse.

Intermediary Liability and Platform Responsibility

The regulation of online violence against women increasingly depends not only on the conduct of individual perpetrators but also on the role played by digital intermediaries such as social media platforms, messaging services, video-sharing websites, search engines, and content-hosting providers. These entities control the architecture through which harmful content is created, amplified, recommended, and removed. As a result, contemporary cyber jurisprudence has shifted from an exclusive focus on criminal liability of users toward a broader inquiry into platform responsibility, due diligence, and accountability. Indian courts have been required to determine the extent to which intermediaries may be obliged to assist victims, remove unlawful content, preserve evidence, and cooperate with investigative authorities while simultaneously protecting freedom of expression and avoiding excessive private censorship.⁵⁰

The foundational statutory framework is contained in Section 79 of the Information Technology Act, 2000, which grants conditional safe-harbour protection to intermediaries for third-party content. The provision reflects the principle that platforms should not automatically be held liable for every piece of user-generated content, as such liability could make digital communication practically impossible. However, the immunity is not absolute. It is subject to the intermediary observing due diligence and acting upon lawful directions relating to unlawful content. Judicial interpretation of these conditions has been central to the development of Indian intermediary liability jurisprudence.⁵¹

A landmark decision in this area is *ShreyaSinghal v Union of India*, where the Supreme Court clarified that intermediaries are not required to remove content merely upon receiving private complaints. The Court held that the obligation to disable access arises when the intermediary receives a court order or a notification from the appropriate government authority relating to unlawful content. This interpretation was intended to prevent intermediaries from engaging in excessive censorship out of fear of liability. At the same time, the judgment preserved the possibility of lawful removal where content falls within constitutionally permissible restrictions or violates valid statutory provisions.⁵²

From the perspective of online violence against women, *ShreyaSinghal* creates both protections and challenges. It protects women's own online expression from arbitrary takedowns triggered by private complaints, but it may also slow the removal of harmful content when victims must first approach courts or governmental authorities. Scholars

⁴⁷Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Rule 3(2)(b).

⁴⁸National Commission for Women, Report on Online Abuse and Cyber Crime against Women p. 71 (NCW, New Delhi, 2022).

⁴⁹Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians p. 50 (Government of India, 2018).

⁵⁰Information Technology Act 2000, s 2(1)(w).

⁵¹Information Technology Act 2000, s 79.

⁵²*ShreyaSinghal v Union of India* (2015) 5 SCC 1, para 117.

have therefore debated whether the judgment, while crucial for free speech, leaves gaps in the context of rapidly spreading image-based abuse and harassment. The tension between procedural safeguards and urgent victim protection remains a defining feature of Indian intermediary law.⁵³

Subsequent regulatory developments, particularly the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, have imposed more detailed due diligence obligations on intermediaries. These include requirements relating to grievance redressal, acknowledgment of complaints, removal of certain categories of unlawful content, preservation of information, and cooperation with law enforcement agencies. For women affected by non-consensual intimate imagery, impersonation, or sexual harassment, the rules provide a potentially faster administrative mechanism for seeking removal of harmful content. However, concerns have also been raised regarding transparency, over-removal, and the concentration of discretionary power in both platforms and the executive.⁵⁴

Indian courts have increasingly emphasized the need for expeditious removal of sexually explicit and privacy-violating content. In cases involving intimate images, fake profiles, and online harassment, High Courts have directed intermediaries to disable access to specific content and assist investigative agencies. Judicial reasoning in these cases often reflects a preventive orientation: because digital harm can multiply through repeated sharing, delay in removal may substantially aggravate the injury suffered by the victim. The focus is therefore not only on punishing the offender but also on minimizing the continued circulation of harmful material.⁵⁵

A particularly difficult issue concerns the distinction between publisher liability and facilitative responsibility. Traditional media entities exercise editorial control before publication, whereas many online platforms host enormous volumes of user-generated content. Courts have generally been reluctant to treat intermediaries as publishers in the conventional sense, but they have increasingly recognized that platforms possess significant technological capacities to detect, restrict, recommend, or demote content. Contemporary scholarship argues that algorithmic amplification and recommendation systems may contribute to the spread of misogynistic abuse, coordinated harassment, and non-consensual imagery, thereby raising questions about whether neutrality remains an adequate description of platform behavior.⁵⁶

The problem becomes more acute in relation to encrypted and cross-platform communication. Harmful content may originate on one platform, be mirrored on several others, and continue circulating through private groups or encrypted channels. Judicial orders directed at a single intermediary may therefore provide only partial relief. Victims often face the burden of pursuing multiple takedown requests across different services, while content can reappear through reposting and screenshotting. Scholars have described this as the problem of persistent digital replication, which challenges the effectiveness of traditional injunctive remedies.⁵⁷

Comparative developments have also influenced Indian debates. Jurisdictions such as the European Union have moved toward stronger platform accountability for illegal content, while maintaining procedural safeguards for users. Indian constitutional scholars caution, however, that importing foreign models without considering India's constitutional commitment to free expression and due process may produce unintended consequences. The challenge is to design a framework that is rights-protective for both victims and speakers, recognizing that excessive censorship and inadequate protection can each undermine constitutional values.⁵⁸

Another emerging concern is the role of intermediaries in responding to AI-generated sexual content and deepfakes. Existing legal frameworks were developed largely for user-uploaded content, but generative AI systems can create fabricated intimate images at scale. Questions arise regarding notice obligations, automated detection tools, watermarking, traceability, and responsibility for synthetic content generated through platform-integrated AI features. Indian jurisprudence has not yet developed a comprehensive approach to these issues, making this one of the most significant future areas of constitutional and cyber law adjudication.⁵⁹

The evolving Indian approach suggests that intermediary liability is gradually moving from a model of passive immunity to conditional accountability. Courts increasingly expect platforms to maintain grievance mechanisms, cooperate with investigations, preserve evidence, and respond to lawful removal requests, particularly in cases

⁵³Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* p. 198 (Oxford University Press, New Delhi, 2016).

⁵⁴Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Rule 3.

⁵⁵*X v State of Maharashtra*, 2021 SCC OnLineBom 458, para 24.

⁵⁶Ministry of Electronics and Information Technology, Annual Report 2023–24 p. 112 (Government of India, 2024).

⁵⁷Law Commission of India, Report No. 267 on Hate Speech p. 89 (2017).

⁵⁸Aparna Chandra, "Consent, Privacy and Digital Sexual Violence" (2025) 17 NUJS Law Review 112, 132.

⁵⁹Ministry of Electronics and Information Technology, Advisory on AI and Deepfake Regulation p. 6 (Government of India, 2024).

involving sexual abuse, privacy violations, and harassment of women. At the same time, constitutional concerns about overbroad censorship, lack of transparency, and private control over public discourse continue to shape judicial caution. The future of platform responsibility in India will likely depend on the development of a more coherent framework that integrates privacy, dignity, freedom of expression, procedural fairness, and technological feasibility within a single constitutional vision of digital governance.

Access to Justice, Investigation and Victim Protection

The effectiveness of judicial protection against online violence against women depends not only on constitutional interpretation or substantive criminal law but also on the practical accessibility of remedies. A legal system that formally recognizes privacy, dignity, and autonomy may still fail victims if complaints are not registered, evidence is not preserved, content is not removed in time, or proceedings become excessively burdensome. In the context of cyber offences, access to justice involves a combination of procedural rights, institutional responsiveness, technological capacity, and victim-sensitive practices. Indian courts have increasingly acknowledged that digital harms require speed, coordination, and specialized expertise, because delay can substantially magnify the injury suffered by victims.⁶⁰

One of the foundational judicial developments in this regard is the Supreme Court's decision in *Lalita Kumari v Government of Uttar Pradesh*, which held that registration of a First Information Report is mandatory when information discloses the commission of a cognizable offence. Although the case was not specific to cybercrime, it has significant implications for online harassment, cyberstalking, image-based abuse, and digital extortion. Victims of online violence have frequently reported reluctance on the part of law-enforcement authorities to treat digital abuse as a serious offence. The principle established in *Lalita Kumari* strengthens the procedural entitlement of victims to have cognizable cyber offences formally registered and investigated.⁶¹

Investigation of online violence presents distinctive evidentiary challenges. Digital content may be deleted, encrypted, mirrored across multiple platforms, or stored on servers located outside India. Effective investigation therefore requires prompt preservation of electronic records, collection of metadata, identification of IP addresses, recovery of deleted material, and cooperation from intermediaries. Courts have increasingly emphasized the importance of preserving digital evidence at the earliest stage, particularly in cases involving intimate images, fake profiles, and persistent online harassment. Failure to act promptly may result in irreversible loss of evidence and continued circulation of harmful content.⁶²

The jurisprudence on electronic evidence has become particularly important for cybercrime prosecutions. In *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, the Supreme Court clarified the requirements for admissibility of electronic records and reaffirmed the importance of certification under the evidentiary framework. With the transition to the *Bharatiya Sakshya Adhiniyam, 2023*, electronic records continue to occupy a central place in criminal adjudication. For victims of online violence, however, strict evidentiary requirements can create practical difficulties, especially when content is rapidly removed or when victims have access only to screenshots rather than original digital records. Scholars have therefore argued for investigative protocols that reduce the evidentiary burden on victims while preserving reliability and authenticity.⁶³

Victim protection is another crucial dimension of access to justice. Courts have increasingly recognized that women subjected to online sexual abuse may face secondary victimization during investigation and trial. Public disclosure of identity, repeated exposure to intimate material, insensitive questioning, and prolonged proceedings can aggravate psychological harm. In response, courts have adopted measures such as protecting the identity of victims, conducting proceedings with sensitivity, and directing authorities to prevent further dissemination of harmful content. These measures reflect a broader constitutional commitment to dignity and privacy in criminal procedure.⁶⁴

The need for rapid content removal has emerged as a recurring judicial concern. In cases involving non-consensual intimate images or sexually explicit material, the injury often continues for as long as the content remains accessible online. Courts have therefore increasingly directed intermediaries to disable access to specific content and assist investigative agencies. Nevertheless, practical limitations remain substantial because content may be reposted, mirrored, or shared through encrypted channels. Judicial orders may reduce the spread of harmful material but do not always guarantee complete erasure from the digital ecosystem.⁶⁵

⁶⁰ Constitution of India, arts 14 and 21.

⁶¹ *Lalita Kumari v Government of Uttar Pradesh* (2014) 2 SCC 1, para 111.

⁶² Ministry of Home Affairs, *Cyber Crime Investigation Manual* p. 78 (Government of India, 2024).

⁶³ *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1, para 65.

⁶⁴ *State of West Bengal v Animesh Boxi*, 2018 SCC OnLine Cal 3182, para 32.

⁶⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Rule 3(2)(b).

Specialized institutional mechanisms have also become important. Cybercrime police stations, digital forensic laboratories, online complaint portals, and specialized investigative units are intended to improve the handling of technology-related offences. The Ministry of Home Affairs' cybercrime reporting portal has expanded the avenues through which victims can lodge complaints, particularly in cases involving women and children. However, empirical studies indicate uneven implementation across states, variations in technical capacity, and limited awareness among victims regarding available remedies. Access to justice therefore remains strongly influenced by geography, resources, and institutional competence.⁶⁶

Another significant challenge is the cross-border nature of digital offences. Perpetrators may operate from different jurisdictions, use virtual private networks, employ anonymous accounts, or rely on foreign-hosted services. Mutual legal assistance procedures are often slow, and differences between national legal systems can hinder investigation and prosecution. Courts have occasionally highlighted the need for greater international cooperation in cybercrime matters, but the existing framework remains cumbersome for victims seeking timely relief. This problem is particularly acute in cases involving large-scale dissemination of intimate content or coordinated transnational harassment campaigns.⁶⁷

Access to justice must also be evaluated through the lens of economic and psychological barriers. Victims may incur legal expenses, lose employment opportunities, require psychological counselling, or withdraw from educational and professional activities. Traditional criminal proceedings rarely address these broader consequences. Scholars have therefore advocated for a more holistic remedial framework including compensation, counselling services, digital safety assistance, and long-term support mechanisms. Comparative research suggests that effective responses to technology-facilitated gender violence require integration of criminal justice with social and psychological support systems.⁶⁸

Despite important judicial advances, significant gaps persist. Investigative delays, limited forensic resources, inconsistent police training, procedural complexity, and fragmented remedies continue to weaken the effectiveness of legal protection. Courts have increasingly recognized these deficiencies, but judicial directions alone cannot substitute for systemic institutional reform. The constitutional promise of dignity and privacy becomes meaningful only when victims can obtain timely, affordable, and effective remedies capable of stopping ongoing harm and facilitating recovery. Indian jurisprudence is gradually moving toward this understanding, yet the realization of genuine access to justice in cases of online violence against women remains an unfinished project requiring coordinated judicial, legislative, administrative, and technological reform.⁶⁹

Critical Evaluation of Judicial Response

The judicial response to online violence against women in India reflects a significant constitutional and doctrinal evolution, yet its effectiveness remains uneven when examined from the perspective of substantive protection, institutional implementation, and technological adaptability. Courts have progressively expanded the scope of privacy, dignity, and autonomy, recognized the seriousness of cyberstalking and image-based abuse, and imposed conditional responsibilities on intermediaries. However, the existence of progressive jurisprudence does not automatically ensure meaningful protection for victims. A critical evaluation requires distinguishing between normative advances in constitutional reasoning and practical limitations in enforcement.⁷⁰

One of the strongest features of Indian judicial response is the adoption of a rights-based approach. The recognition of informational privacy in *Justice K.S. Puttaswamy (Retd.) v Union of India* transformed the constitutional understanding of digital harms by linking control over personal information to dignity and autonomy. This development allows courts to treat non-consensual dissemination of intimate images, digital impersonation, and intrusive surveillance as violations of constitutional rights rather than merely technical offences. Scholars have rightly described this as a shift from a morality-centered framework to an autonomy-centered framework, which is particularly important for women whose digital identities are often targeted through gendered forms of abuse.⁷¹

Judicial protection of freedom of expression has also been a notable achievement. In *Shreya Singhal v Union of India*, the Supreme Court prevented the use of vague and overbroad criminal provisions that could have chilled legitimate online speech. This is especially relevant for women activists, journalists, and political participants who may otherwise

⁶⁶Ministry of Home Affairs, National Cyber Crime Reporting Portal: Annual Report p. 45 (Government of India, 2025).

⁶⁷Parliamentary Standing Committee on Home Affairs, *Capacity Building for Cyber Crime Investigation* p. 92 (Rajya Sabha Secretariat, New Delhi, 2025).

⁶⁸National Commission for Women, *Report on Cyber Crime against Women* p. 74 (NCW, New Delhi, 2022).

⁶⁹Mrinal Satish and Aparna Chandra, "Technology-Facilitated Gender Violence and the Limits of Indian Criminal Law" (2024) 15 Indian Law Review 221, 238.

⁷⁰Constitution of India, arts 14, 19 and 21.

⁷¹Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1, para 297.

be vulnerable to selective censorship. The judgment demonstrates a commitment to constitutional proportionality and procedural safeguards, ensuring that regulation of online content remains subject to constitutional scrutiny.⁷²

At the same time, the jurisprudence reveals a structural tension between free speech and victim protection. The requirement that intermediaries act upon court orders or governmental notifications may provide due process safeguards, but it can also delay the removal of rapidly spreading harmful content. In cases of image-based abuse, hours or days may be crucial. Scholars have therefore questioned whether the current framework adequately responds to the speed and scale of digital dissemination. The legal system continues to struggle with designing procedures that are both constitutionally protective and practically effective.⁷³

A further limitation is the fragmented nature of the substantive legal framework. Online violence against women is currently addressed through a combination of provisions relating to stalking, obscenity, privacy, intimidation, extortion, defamation, and intermediary regulation. Courts have attempted to harmonize these provisions through constitutional interpretation, but the absence of a dedicated and comprehensive statute on technology-facilitated gender-based violence creates doctrinal inconsistency. Similar forms of harm may be analyzed under different legal categories depending on the facts of the case, leading to uncertainty in prosecution and adjudication.⁷⁴

The judicial response has also been predominantly reactive rather than preventive. Most remedies become available only after the harm has occurred and often after the content has already circulated widely. Even successful takedown orders may not fully eliminate the material from the digital ecosystem because of reposting, mirroring, screenshots, and cross-platform dissemination. This exposes a fundamental limitation of traditional legal remedies when applied to networked technologies. Courts can order removal, but they cannot easily restore the pre-violation condition of privacy and reputation.⁷⁵

Institutional capacity remains another major concern. Judicial sensitivity has not always been matched by police responsiveness, forensic capability, or prosecutorial efficiency. Empirical studies and committee reports repeatedly highlight delays in registration of complaints, inadequate understanding of cyber offences, difficulties in preserving electronic evidence, and limited cooperation between agencies. Victims often face multiple proceedings for criminal prosecution, content removal, and compensation, increasing the emotional and financial burden of seeking justice. The gap between constitutional promise and institutional delivery continues to weaken the practical impact of judicial advances.⁷⁶

The treatment of psychological and social harm also remains underdeveloped. Courts have acknowledged emotional distress and reputational injury, but remedies are still largely framed within criminal law. Compensation, counselling, digital safety assistance, and long-term rehabilitative measures receive comparatively less attention. Feminist scholars argue that technology-facilitated gender violence should be understood not only as individual wrongdoing but also as a mechanism that restricts women's participation in public life. From this perspective, effective remedies must address the broader consequences of exclusion, fear, and self-censorship.⁷⁷

Another area requiring critical scrutiny is platform accountability. Indian courts have moved toward conditional intermediary responsibility, yet the deeper issue of algorithmic amplification has received limited judicial attention. Contemporary research shows that recommendation systems, engagement-driven ranking, and automated amplification can intensify misogynistic abuse and coordinated harassment. Current jurisprudence focuses largely on notice-and-takedown obligations rather than on the structural role of platform design in facilitating harmful content. As digital communication becomes increasingly algorithmic, this gap may become more significant.⁷⁸

The emergence of AI-generated deepfakes and synthetic sexual content further exposes the limitations of existing jurisprudence. Traditional doctrines were developed for authentic user-generated content, whereas generative AI can create fabricated intimate material at scale. Indian courts have not yet articulated a comprehensive constitutional framework for addressing synthetic sexual violence, including questions of attribution, platform responsibility, evidentiary standards, and preventive regulation. Future judicial development in this area will be crucial for

⁷² Aparna Chandra, "Consent, Privacy and Digital Sexual Violence" (2025) 17 NUS Law Review 112, 120.

⁷³ *ShreyaSinghal v Union of India*, (2015) 5 SCC 1, para 87.

⁷⁴ Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* p. 198 (Oxford University Press, New Delhi, 2016).

⁷⁵ MrinalSatish and Aparna Chandra, "Technology-Facilitated Gender Violence" (2024) 15 Indian Law Review 221, 236.

⁷⁶ Ministry of Electronics and Information Technology, *Annual Report 2023–24* p. 112 (Government of India, 2024).

⁷⁷ Parliamentary Standing Committee on Home Affairs, *Capacity Building for Cyber Crime Investigation* p. 88 (Rajya Sabha Secretariat, New Delhi, 2025).

⁷⁸ National Commission for Women, *Cyber Crime Prevention and Awareness Report* p. 61 (NCW, New Delhi, 2023).

determining whether existing principles of privacy, dignity, and autonomy can effectively respond to rapidly evolving technologies.⁷⁹

Despite these limitations, it would be inaccurate to conclude that the judicial response has been ineffective. The cumulative effect of decisions relating to privacy, dignity, cyberstalking, image-based abuse, and intermediary responsibility has created a substantially stronger constitutional foundation for protecting women in digital spaces than existed a decade ago. Courts have increasingly recognized that online violence is not a trivial or purely virtual phenomenon but a form of real harm capable of affecting equality, autonomy, reputation, mental health, and democratic participation. The jurisprudence is therefore best understood as progressive but incomplete: it has established important constitutional principles, yet it has not fully resolved the institutional, technological, and structural challenges posed by contemporary digital environments.⁸⁰

A more effective future framework would require closer integration of constitutional rights, criminal law, data protection, platform governance, and victim support mechanisms. Judicial innovation has opened the path toward such an integrated approach, but the realization of meaningful protection against online violence against women will ultimately depend on coordinated reforms extending beyond the courtroom.

CONCLUSION

The judicial response to online violence against women in India reflects a significant evolution in constitutional interpretation within the digital age. The judiciary has played a transformative role in expanding the scope of fundamental rights to address emerging challenges posed by cyberspace, particularly those affecting women's dignity, privacy, and autonomy. Through progressive interpretations of Articles 14, 19, and 21 of the Constitution, courts have recognised that the protection of fundamental rights must extend beyond physical spaces and operate effectively within digital environments.

Landmark judgments have established that the right to privacy, dignity, and informational autonomy are integral components of the right to life and personal liberty. Judicial recognition of these rights has provided a strong constitutional foundation for addressing cyberstalking, online harassment, non-consensual dissemination of intimate images, digital impersonation, and morphing. At the same time, the judiciary has sought to maintain a delicate balance between safeguarding freedom of speech and preventing its misuse as a tool for harassment, abuse, and exploitation in online spaces.

Furthermore, judicial decisions have clarified the role and responsibilities of intermediaries, emphasising the need for due diligence and timely removal of unlawful content. The courts have also contributed to strengthening victim protection by recognising the severe psychological, reputational, and social consequences of online abuse. In doing so, they have underscored that online violence against women is not merely a technological issue but a serious violation of constitutional and human rights.

However, despite these progressive developments, certain limitations remain. Judicial interventions are often reactive in nature and depend on cases being brought before the courts. The absence of comprehensive and specialised legislation addressing emerging forms of cyber violence, such as deepfakes and advanced image manipulation, continues to pose challenges. Additionally, issues relating to enforcement, delays in judicial processes, and difficulties in cross-border investigations limit the effectiveness of judicial remedies. To effectively neutralize internet-based abuse, the courts must transition from simple legal arbiters into active protectors of fundamental rights within digital environments. While multiple statutes touch upon digital offenses, their real-world impact depends heavily on whether judges evaluate cyber-harm with proper gender awareness, recognizing that virtual violation inflicts severe, tangible damage on a person's life. The judiciary plays a critical role in bridging the gap between rigid, lagging legislation and fast-evolving technology by mandating rapid content takedowns, penalizing abusers and keeping social media companies accountable. True digital safety is not achieved by telling women to restrict their online activity, but by using the law to break down the digital ecosystem of impunity that shields online harassers. A tech-literate, sensitive judicial standard is crucial to building a secure, inclusive web where women can safely exercise their own voices without facing digital exclusion.

⁷⁹Information Technology Act 2000, s. 79.

⁸⁰Ministry of Electronics and Information Technology, *Advisory on Deepfake and AI Generated Content* p. 6 (Government of India, 2024).