IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

Judicial Interpretation and Enforcement Challenges in Addressing Cyber Crimes Against Women in India

Jyoti Chandel
Department of Law, Samrat Vikramaditya Vishwavidyalaya, Ujjain
Dr. Aruna Sethi
Professor, Government Law College, Ujjain

Abstract: *The rapid growth of internet use in India has been accompanied by a worrying surge in cyber crimes targeting women. This paper examines how the Indian judiciary has interpreted and applied laws to address online violence against women, and the challenges faced in enforcing those laws. It outlines the legal framework – including key provisions of the Information Technology Act 2000 and the Indian Penal Code – and analyzes landmark judgments such as Shreya Singhal v. Union of India (2015), which struck down the overbroad Section 66A of the IT Act, Kirti Vashisht v. State (Delhi HC, 2019), which instituted "Zero FIR" for cyber offences, and X v. Union of India (Madras HC, 2025), which established robust takedown mechanisms for intimate images. Despite these legal tools and progressive court interventions, enforcement on the ground remains fraught with technical hurdles, jurisdictional issues, under-reporting, and police apathy. The analysis reveals significant gaps between laws on paper and their implementation. The paper concludes with recommendations for a more gender-sensitive cyber enforcement regime – including legal reforms, specialized investigative units, better inter-agency coordination, and victim-centric procedures – to ensure that women's rights to safety, privacy, and dignity are better protected online.*

Keywords: Cyber Crimes Against Women; Online Harassment; Information Technology Act 2000; Judicial Activism; Enforcement Challenges; Digital Safety

I. INTRODUCTION

Cyber crimes against women in India span a wide array of digital offenses including online harassment, cyberstalking, impersonation, defamation, voyeurism, and the non-consensual sharing of intimate images ("revenge porn"). These crimes leverage the anonymity and expansive reach of the internet, often amplifying existing misogynistic norms. NCRB data indicates a troubling rise: 17,950 cyber crimes against women were recorded in 2021—a 16.8% increase over the previous year—and over 2,250 cases of explicit content dissemination were documented in 2022. However, these figures significantly underrepresent reality; a National Commission for Women study found that 54.8% of women had faced online abuse, yet most incidents remain unreported due to stigma and lack of institutional trust.

To address this, Indian lawmakers have enacted provisions under the Information Technology Act, 2000 and the Indian Penal Code. Government initiatives like the Cyber Crime Reporting Portal, CCPWC scheme, and the proposed Bharatiya Nyaya Sanhita aim to modernize legal responses to digital harms. Yet, victims continue to face barriers such as unclear legal definitions, inadequate policing, and delays in justice.

This paper adopts a doctrinal and analytical approach to examine judicial interpretations of cyber laws affecting women. It explores three core questions: Do current laws sufficiently protect women from cyber violence? How have Indian courts expanded these protections through precedent? And what enforcement challenges remain? Through legal analysis, case studies, and empirical data, the paper critically evaluates gaps in enforcement and proposes reforms—legislative, judicial, and institutional—to better uphold women's digital rights to privacy, dignity, and safety.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

II. REVIEW OF LITERATURE

Early academic research on cyber crimes against women in India highlights a concerning gap between the rapid evolution of digital technologies and the sluggish development of corresponding legal safeguards. Indian law still lacks a unified statutory definition of "cybercrime." Instead, a range of provisions under the Information Technology Act, 2000 and the Indian Penal Code (IPC) are applied to cover offenses involving digital platforms. Scholars generally categorize cyber crimes as either "cyber-enabled" — traditional crimes like harassment or stalking executed via digital means — or "cyber-dependent," such as hacking or data theft. Legal responses tend to lag behind new technological harms, such as AI-generated deepfakes or social media doxxing.

Feminist scholarship emphasizes that patriarchal norms underpinning offline violence are reproduced and amplified in digital spaces. Ahlawat and Sharma (2024) note that Indian women encounter a continuum of risks online — from obscene messages and trolling to coordinated doxxing campaigns — echoing societal power imbalances. Ironically, internet features meant to empower users — anonymity and global access — are also exploited for abuse. Yadav (2022) documents the prevalence of cyberstalking and revenge porn but notes that victims are reluctant to seek legal recourse, citing stigma and distrust in police responsiveness. The National Commission for Women has similarly reported that more than half of Indian women internet users have faced harassment, but few file formal complaints.

Empirical data supports these concerns. NCRB's *Crime in India 2022* report shows an 11% rise in cyber crimes against women, with over 2,250 cases of transmitting sexually explicit content and 689 other gendered cyber offenses. However, under-reporting remains rampant. A 2023 Internet Freedom Foundation study revealed that nearly 68% of victims never report cyber harassment, fearing humiliation or dismissal by authorities.

Scholars also critique the fragmented and outdated legal framework. Before the Criminal Law (Amendment) Act, 2013, cyberstalking lacked specific recognition. Even now, overlapping provisions under the IPC and IT Act create confusion — for instance, whether a morphed intimate image should be prosecuted under obscenity, defamation, or both. Trisha Shreyashi (2024) notes that the current mix of laws, including the new Digital Personal Data Protection Act (2023), still fails to offer a consolidated framework or clear definitions.

Judicial interpretation has somewhat filled these gaps. High Courts have recognized a "right to be forgotten" in cases of non-consensual image sharing. In *Subhranshu Rout v. State of Odisha* (2020), the Orissa High Court upheld the victim's right to privacy and denied bail to the accused. Still, such progress remains case-specific and reactive, highlighting the need for a cohesive doctrinal and enforcement framework moving forward.

Legal Framework

Statutory Provisions: The response to cyber crimes against women in India rests primarily on two legal pillars: the Indian Penal Code, 1860 (IPC) and the Information Technology Act, 2000 (IT Act). Together, these laws provide the principal framework for criminalizing online offenses targeting women, though gaps and overlaps exist. The IPC – a general criminal code – has been amended in recent decades to address gender-based violence and some cyber behaviors, while the IT Act is a special law focused on electronic offenses. Key IPC sections relevant to online abuse include: Section 354D (stalking, including monitoring a woman's online activity), Section 509 (word, gesture or act intended to insult a woman's modesty, used for sexual harassment including online abuse), Section 500 (criminal defamation, applicable to defamatory content posted online), Section 354A (sexual harassment, which can cover unwelcome sexual advances via electronic communication), Section 354C (voyeurism, criminalizing capture or sharing of images of a woman's private act without consent – relevant to secretly filmed content uploaded online), and Section 507 (criminal intimidation by anonymous communication, often invoked for rape or death threats sent via anonymous emails or social media). The IT Act 2000 (amended in 2008) specifically addresses crimes involving electronic communication. Notable provisions include: Section 66A (sending offensive messages via electronic means) – introduced in 2009 but **struck down in 2015** as unconstitutional for vagueness and overbreadth; Section 67 (publishing or transmitting obscene material in electronic form) – used to prosecute online obscenity and non-consensual sharing of nude or sexual images (punishable by up to 3 years for first conviction); Section 67A (publishing or transmitting sexually explicit material) – targeted at more explicit pornographic content, including revenge porn, with higher penalties (5 to 7 years); and Section 66E (violation of privacy by capturing or sharing private images without consent,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

e.g. "voyeuristic" images, punishable by up to 3 years). These provisions are supplemented by others (like IT Act Section 67B against child pornography, and various procedural sections in the Code of Criminal Procedure). Additionally, constitutional rights – particularly Article 21 of the Constitution, protecting life and personal liberty – provide a backdrop, as courts have interpreted Article 21 to safeguard privacy and dignity, which are implicated in cases of online abuse of women.

Evolution and Interpretation: The legal framework has evolved through both legislative action and judicial decisions. A watershed moment was *Shreya Singhal v. Union of India* (Supreme Court, 2015), where the Court struck down Section 66A of the IT Act for violating freedom of speech. While this judgment was celebrated for upholding constitutional rights, it inadvertently removed a tool that law enforcement had frequently (and sometimes improperly) used against online harassment. After *Shreya Singhal*, there was concern that victims of cyberbullying and abuse lost a quick recourse, since 66A had been a catch-all provision for online threats and insults. The government did not immediately replace 66A with a narrower law, instead leaning on existing IPC sections and improving reporting mechanisms (like the cybercrime portal). Meanwhile, repeated misuse of 66A by police even after its invalidation led the Supreme Court to issue advisories directing authorities not to register cases under the defunct section, highlighting gaps in police awareness. Another legislative development was the 2013 amendment to the IPC (post the *Nirbhaya* case and Justice Verma Committee recommendations), which, among other things, introduced Section 354D (for stalking) and strengthened laws on sexual harassment and voyeurism, thereby covering some online behaviors that previously had no specific provision. More recently, as noted, the draft Bharatiya Nyaya Sanhita bill (2023) aims to modernize the IPC, including explicit recognition of cyber offences targeting women.

Table 1 below summarizes some **key legal provisions** addressing cyber crimes against women in India, along with their scope and penalties:

Legal Provision	Scope of Offense (relevant to cyber context)	Penalty
IPC §354D (Stalking)	Following or contacting a woman repeatedly, including monitoring her internet use (covers cyberstalking).	Up to 3 years (1st offense); up to 5 years (repeat).
IPC §509 (Insulting modesty)	Words/gestures intended to insult a woman's modesty (used for online sexual harassment, trolling).	Up to 3 years and fine.
IPC §500 (Defamation)	Publishing any defamatory imputation (applies to libelous social media posts, morphed images harming reputation).	Up to 2 years and fine.
IPC §354C (Voyeurism)	Capturing or sharing images of a woman's private act without consent (covers secretly filming and distributing content).	1–3 years (first offense); 3–7 years (subsequent).
IPC §507 (Anon. criminal threats)	Criminal intimidation via anonymous communication (relevant for rape/death threats sent from unknown online accounts).	Up to 2 years (in addition to punishment for intimidation).
IT Act §66A (struck down)	Sending "grossly offensive" or menacing messages via electronic communication (used for online abuse; struck down in 2015 as unconstitutional).	N/A (struck down).
IT Act §67 (Obscenity)	Publishing/transmitting obscene material in electronic form (used for non-consensual sharing of nude images, etc.).	Up to 3 years + fine (first conviction); up to 5 years (subsequent).
IT Act §67A (Sexually explicit)	Publishing/transmitting material containing explicit sexual acts (covers revenge porn, explicit videos without consent).	Up to 5 years + fine (first); up to 7 years (repeat).
IT Act §66E (Privacy violation)	Capturing or sharing images of a person's private areas without consent (addresses non-consensual imagery that may not be "obscene" but violates privacy).	Up to 3 years or fine up to ₹2 lakhs.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

Indian courts have played a pivotal role in shaping the legal response to cyber crimes against women, especially in the absence of detailed legislative mechanisms. Landmark judgments have interpreted and expanded the scope of existing statutes to provide relief to victims.

In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the Information Technology Act for violating the right to free speech under Article 19(1)(a). However, it left a legislative void regarding online harassment. High Courts stepped in to bridge such enforcement gaps through progressive judicial interventions.

A notable example is *Kirti Vashisht v. State* (Delhi High Court, 2019), where the petitioner, a victim of revenge porn, was denied help due to jurisdictional issues. The Court invoked the concept of "Zero FIR," mandating that any police station receiving a cybercrime complaint must register it irrespective of territorial jurisdiction. This removed a major bureaucratic hurdle and ensured prompt initiation of legal proceedings.

Another important case is *State of West Bengal v. Animesh Boxi* (Barrackpore Trial Court, 2018), one of India's first convictions for non-consensual pornography. The accused uploaded intimate images of his ex-girlfriend on a pornographic website. He was convicted under Section 67A of the IT Act and sentenced to five years' imprisonment. The judgment emphasized the violation of the victim's fundamental rights to privacy and dignity, aligning such digital sexual crimes with the severity of offline sexual offenses.

In *X v. Union of India & Ors.* (Madras High Court, 2025), the judiciary addressed the persistent harm caused by the viral spread of non-consensual intimate images. Despite FIR registration, the videos continued to circulate online. Recognizing this as a breach of Article 21 (right to privacy and dignity), the Court issued a comprehensive Standard Operating Procedure (SOP). It directed the Ministry of Electronics and Information Technology to act on complaints within 48 hours, compelled platforms to remove content within 24 hours or risk losing safe harbor under Section 79 of the IT Act, and urged creation of hash databases to prevent re-uploads. This judgment illustrates the judiciary's proactive stance in remedying legal and enforcement gaps.

III. ANALYSIS AND DISCUSSION

Judicial activism in India has played a pivotal role in shaping the response to cyber violence against women. Landmark rulings such as *Shreya Singhal v. Union of India* (2015) upheld fundamental rights by striking down Section 66A of the IT Act, while urging lawmakers to draft clearer laws to address online abuse. Courts have since adopted victim-centric interpretations, as seen in *Kirti Vashisht v. State* (2019), which emphasized Zero FIR registration, removing jurisdictional barriers. Lower courts like in *Animesh Boxi* (2018) treated revenge porn as a violation of fundamental rights, and *X v. Union of India* (Madras HC, 2025) established innovative systemic remedies, including intermediary accountability and time-bound takedowns.

Despite judicial progress, enforcement remains weak. Under-reporting is rampant due to fear, stigma, and apathy from police. Many complaints are dismissed or trivialized. Even when FIRs are filed, technical hurdles such as tracing anonymous offenders, obtaining platform data, and cross-jurisdictional cooperation impede investigation. Police often lack training in digital forensics, and there is a shortage of cyber forensic labs.

Legal ambiguities persist, with overlapping IPC and IT Act provisions leading to confusion. Absence of specific laws on emerging threats like cyberbullying, doxxing, or deepfake abuse forces reliance on outdated statutes. Inter-state and international cooperation is slow and fragmented, making enforcement harder.

Nevertheless, improvements exist. Specialized cyber police stations and women-centric helpdesks have emerged. Courts monitor sensitive cases, and public awareness is growing. However, conviction rates remain low due to evidentiary and procedural issues.

In conclusion, while Indian courts have driven progressive legal interpretations, systemic enforcement gaps persist. Bridging this divide requires stronger institutional coordination, legislative updates, enhanced training, and better victim support mechanisms to ensure digital safety and dignity for women.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

IV. FINDINGS

The critical examination above yields several findings about the current state of legal responses to cyber crimes against women in India:

Growing Legal Recognition, But Persistent Gaps: There is growing legal recognition of online gender-based violence as a serious issue – evidenced by new statutes (2013 IPC amendments, proposed 2023 bill) and progressive court rulings. However, significant gaps remain. The law is often reactive and piecemeal; definitions of cyber offences are scattered or incomplete, leaving some harmful behaviors (like coordinated online harassment or image-based abuse using new technologies) not squarely addressed. The absence of a unified cybercrime framework leads to inconsistent application and confusion in enforcement agencies.

Judiciary as a Catalyst: The judiciary has acted as a catalyst for reform and relief. Landmark cases have expanded victims' access to justice (e.g., Zero FIR in *Kirti Vashisht*) and innovated remedies (takedown protocols in *X v. UOI*). Courts have affirmed that online abuse of women implicates fundamental rights to equality, dignity, and privacy, thereby framing it as a constitutional concern, not just a criminal law issue. Nonetheless, judicial action has been case-specific; a comprehensive jurisprudence or consistent doctrine is still evolving. The proactive measures seen in some High Court judgments are not yet institutionalized nationwide.

Enforcement Deficit: A clear finding is the *enforcement deficit* – i.e., the discrepancy between laws on the books and outcomes on the ground. Official data and studies confirm widespread under-reporting and under-enforcement. Many victims do not enter the legal system at all due to fear or skepticism towards authorities. Even for those who do, police responses can be lacking – from failure to register cases (prior to reforms like Zero FIR) to inadequate investigation efforts. Technical challenges such as anonymity of offenders and cross-border jurisdiction issues further hinder enforcement, as does the limited capacity of police and forensics labs. These issues result in relatively few cases progressing to successful prosecutions, which in turn reduces the deterrent effect of the law.

Need for Multi-Pronged Reforms: The analysis highlights that no single intervention will suffice; a multi-pronged approach is needed. Legal reforms must clarify and strengthen provisions related to cyber harassment and abuse. Law enforcement agencies need better training, resources, and accountability to handle cyber crimes against women with urgency and sensitivity. Intermediaries (social media platforms, websites) are key players in the digital ecosystem and must be more accountable in promptly removing abusive content and assisting investigations. Victim support systems (such as helplines, counseling, legal aid) are also crucial to encourage reporting and help survivors navigate the process.

In essence, while India has made strides in acknowledging and legislating against cyber violence targeting women, the findings reveal a **pronounced implementation gap**. Bridging this gap is essential to turn legal provisions and court pronouncements into actual protection for women in cyberspace.

V. CONCLUSION AND SUGGESTIONS

Cyber crimes against women in India reflect deep-rooted misogyny reshaped through digital platforms. While legal frameworks and judicial decisions have addressed these harms, enforcement remains inconsistent. To bridge the gap between law and justice, legislative reforms must clarify and expand definitions for online abuse, including doxxing and cyberbullying, while codifying a right to be forgotten. Law enforcement agencies should be strengthened through cybercrime units, regular training, and accountability measures. Judicial reforms are equally essential—special courts, in-camera trials, and judicial sensitivity training will improve access to justice. Collaboration with tech platforms is critical for swift takedown of abusive content and offender identification. Finally, accessible victim support systems and public awareness campaigns will empower women to report abuse without fear. Achieving a safer cyberspace for women demands holistic action from lawmakers, courts, agencies, and society, ensuring the constitutional ideals of equality, dignity, and privacy are upheld in the digital era.

REFERENCES / BIBLIOGRAPHY

[1]. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India) – Struck down IT Act §66A as unconstitutional.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

[2]. Kirti Vashisht v. State & Ors., CRL.M.C. 5933/2019 (Delhi High Court, Judgment dated 29 Nov 2019) – Directed police to register "Zero FIR" for cyber offences irrespective of jurisdiction.

[3]. State of West Bengal v. Animesh Boxi, C. Case No. 25/2017 (WB Trial Court, 29 Mar 2018) – First conviction for non-consensual pornography (revenge porn); 5-year imprisonment under IT Act §67A.

[4]. X v. Union of India & Ors., W.P. No. 25017/2025 (Madras High Court, Interim Order dated 9 July 2025) – Established SOP for rapid removal of intimate images online and intermediary accountability.

[5]. Subhranshu Rout @ Gugul v. State of Odisha, BLAPL No. 4592/2020 (Orissa High Court, Order dated 22 Dec 2020) – Recognized victim's "right to be forgotten" for intimate images (denied bail to accused in video morphing case).

[6]. **Information Technology Act, 2000 (India)** – Key sections: 66A (offensive messages, **struck down**), 66E (privacy violation), 67 (obscene material), 67A (sexually explicit material).

[7]. **Indian Penal Code, 1860**, as amended by Act 13 of 2013 – Key sections for crimes against women: 354A, 354C, **354D** (stalking, incl. cyberstalking), 499–500 (defamation), 507 (anonymous criminal intimidation), 509 (insult to modesty).

[8]. **Criminal Law (Amendment) Act, 2013** – Introduced offences like stalking (IPC 354D) and voyeurism (IPC 354C) to address emerging crimes, including online variants.

[9]. **National Crime Records Bureau (NCRB)** – Crime in India 2021 and Crime in India 2022 reports (Ministry of Home Affairs, Govt. of India). **2021** report noted 17,950 cyber crimes against women (16.8% rise from 2020); **2022** report showed an 11% further increase, including 2,251 cases of publishing sexually explicit material of women.

[10]. **National Commission for Women (NCW)** – Study on Cyber Harassment Experiences (2020). Found 54.8% of women surveyed experienced online harassment, and 26% had intimate images morphed/shared without consent. Highlighted low reporting due to fear and distrust in authorities.

[11]. Ahlawat, H. & Sharma, S. (2024). "Cyber Crimes Against Women in India." ShodhKosh Journal, 5(6), 1539–1544. (Examines forms of cyber violence and legal responses; notes continuum of online-offline gender violence).

[12]. Yadav, H. (2022). "Unveiling the Dark Side of Cyberspace: A Study of Cyber Crimes Against Women in India." Int'l Journal of Food and Nutritional Sciences, 11(10), 3408–3415. (Documents prevalence of cyberstalking, harassment, revenge porn; discusses legal shortcomings and need for training).

[13]. Citizens for Justice and Peace (CJP) Team. (2025, Nov 5). "Cybercrime and the Crisis of Digital Justice: India's Invisible Victims Online." (Report highlighting that ~68% of Indian cyber-harassment/fraud victims did not report to police; discusses reasons for under-reporting and issues in FIR lodging).

[14]. Indialaw (Shukla, A.). (2025, July 17). "Delete. Block. Report. Repeat No More — Madras HC Brings End to Woman's Online Ordeal." (Blog article summarizing X v. Union of India case and the court-mandated SOP for swift takedowns).

[15]. Pande, A. & Holani, G. (2025, Aug 6). "Humane Judicial Approach to Revenge Porn in India." LiveLaw.in. (Analysis of how courts are handling revenge porn cases; discusses Animesh Boxi and NCRB data on cyber obscenity cases).

[16]. Rajkumar, A. (2023, Dec 5). "Crimes against women rise by 4%, cyber crimes increase by 11%: NCRB data." The News Minute. (News report on NCRB 2022 statistics; notes spike in cyber crimes targeting women).

[17]. Shreyashi, T. (2024, Nov 14). "Will women-centric laws create a safer cyberspace for women?" The Times of India (Blog). (Discusses definitional issues, jurisdiction problems, and outcomes of stakeholder consultations on cyber safety; advocates for legal clarity and better enforcement).