IMPACT OF CYBER LAWS IN PROTECTION OF WOMEN FROM CYBERCRIMES

ARCHANA JOHARI
Research Scholar, Institute of Legal Studies, Shri Ramswaroop Memorial University, Lucknow, Uttar Pradesh, India

DR. SHASHANK SHEKHAR
Associate Professor, Institute of Legal Studies, Shri Ramswaroop Memorial University, Lucknow, Uttar Pradesh, India

ABSTRACT

The rapid expansion of digital technologies in India has transformed social interaction while simultaneously intensifying women's exposure to cybercrimes such as cyberstalking, online harassment, sextortion, identity theft, non-consensual intimate image circulation, and emerging threats like deepfakes. This paper examines the impact of cyber laws in protecting women from cybercrimes through a doctrinal, judicial, and data-driven analysis. It critically evaluates the effectiveness of India's cyber legal framework, including the Information Technology Act, 2000, and the post-2023 criminal law reforms under the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam. Drawing upon NCRB and NCRP data from 2020–2024, the study demonstrates a sharp rise in cyber offences against women alongside improved reporting, charge-sheeting, and institutional responsiveness. Judicial developments, particularly post-Puttaswamy, reveal a constitutional shift in framing cyber violence as violations of dignity, privacy, and equality rather than mere technical offences. However, despite enhanced procedural access, intermediary obligations, and evidentiary reforms, substantive deterrence remains limited due to enforcement gaps, low conviction rates, technological asymmetries, and social stigma. The paper argues that while Indian cyber laws have significantly strengthened women's access to justice and recognition of digital harm, sustained legal, technological, and institutional reforms are essential to translate formal protection into effective deterrence and meaningful safety in cyberspace.

KEYWORDS: Cybercrime, Women, Privacy, Dignity, Enforcement

INTRODUCTION

The high rate of cybercrimes that has been experienced by the Indian society due to rapid digitalisation has imposed a disproportionate impact on the women in society, raising a serious concern on the need to have a stronger legal elucidation. The latest Crime in India 2023 report released by the National Crime Records Bureau reported almost 4.48 lakh cases of crimes against women; this is based on the fact that cyber-based crimes like cyberstalking, harassment, and non-consensual distribution of intimate images are also adding to the crime rate. More broadly, cybercrime has also experienced an explosion: by 2024 it was estimated that reported cases of cybercrime grew over 22 lakh, almost 400 percent higher than they had been in 2021, with offenses such as sextortion, phishing, and online fraud increasing across multiple states, such as Maharashtra, Uttar Pradesh and Karnataka. False reporting and enforcement have been noted to remain a challenge because most women victims are too afraid to report stigma and because of less digital skills, despite growing trends in online abuse being reflected in official figures. The high-profile cases of late like that of a Hyderabad woman who was extorted by fraudulently created obscene videos in 2025 only show how cyber harassment can turn into financial and psychological abuse, highlighting the associated multi-tiered vulnerability of women online. As a natural extension of these issues, the cyber legal frame of India revolving around the Information Technology Act, 2000 and more recently being supplemented by the Bharatiya Nyaya Sanhita, 2023 attempts to target both the traditional and new aspects of digital abuse against women. These legislations are not merely meant to criminalise any explicit cyber crimes, but also to oblige intermediaries and enhance investigative processes. The legal system has expanded the conceptualisation of harm in cyberspace so far as it has shown through the control of legal provisions that have targeted online harassment, invasion of privacy, and online exploitation of individuals beyond the limited technical definition of hate speech to uphold dignity and safety. It is thus imperative to assess the effectiveness of these cyber laws in order to feel how well they can facilitate prevention, promptness as well as redress against women victims of cybercrime and also to gain insight into areas that lack these laws but require improvement of the law and enforcement, to ensure that the law is effective.

JUDICIAL EVOLUTION IN ADDRESSING GENDER-BASED CYBER VIOLENCE IN INDIA

Judicial engagement with cyber laws over the last decade reveals a gradual but clear move towards recognising online gender-based violence as a serious violation of women's dignity, equality and privacy, even though doctrinal and enforcement gaps remain. Courts have repeatedly relied on the Information Technology Act, 2000 (especially Sections 66C, 66D, 66E, 67 and 67A) read with IPC/BNS provisions on outraging modesty, stalking and criminal intimidation, and post-2017 on the fundamental right to privacy under Article 21, to frame cyber harms as constitutional injuries rather than mere technical offences.

In *Shreya Singhal v. Union of India*,[1] the Supreme Court struck down Section 66A IT Act as unconstitutional for vagueness and chilling effect on free speech, but carefully preserved the validity of Section 69A and the blocking rules, thereby balancing expression with targeted state power to remove illegal content including misogynistic and abusive online speech against women. This judgment indirectly shaped cyber-protection jurisprudence for women: while it removed an overbroad tool that was sometimes invoked in complaints by women, it compelled police and courts to fall back on more precise provisions like Sections 66E, 67 and 67A IT Act, and Section 354D IPC (now Section 78 BNS) in cyberstalking and NCII (non-consensual intimate image) cases, encouraging a rights-compatible and narrowly tailored approach to criminalisation.

A constitutional deepening of cyber-protection arose in "*Justice K.S. Puttaswamy v. Union of India'*,[2] where a nine-judge bench affirmed privacy including bodily, decisional and informational privacy as an intrinsic facet of Article 21, explicitly covering digital spaces and data profiles. Subsequent High Court decisions have interpreted cyber voyeurism, doxxing, non-consensual circulation of images and online stalking as invasions of informational privacy and autonomy, thus converting statutory offences under Section 66E IT Act and Section 354C/354D IPC (now BNS Sections 74–78) into direct violations of fundamental rights, strengthening women's claims to injunctive relief, content-takedown orders and more victim-centric procedural accommodations.

The Bulli Bai and Sulli Deals prosecutions (2021–2022) mark a watershed in judicial recognition of communalised misogyny in cyberspace, where Muslim women activists and journalists were 'auctioned' via GitHub-hosted apps using stolen or morphed photographs, triggering FIRs under Sections 153A, 153B, 295A IPC, Sections 354D, 509 IPC and Sections 66, 67 IT Act. Orders of courts in Delhi and Mumbai emphasised that such acts constituted aggravated gendered harassment and hate speech, not mere 'offence to religious feelings' or pranks, and directed robust digital forensics and platform cooperation; yet the grant of bail to multiple accused in 2022, while grounded in due process, has been criticised by scholars and women's groups as undercutting deterrence and signalling judicial leniency in the face of organised online targeting of minority women.

In recent NCII and cyber-harassment matters, such as the Madras High Court's intervention in *X v. Union of India & Ors.* (2024/2025, NCII case concerning intimate images repeatedly resurfacing online), the judiciary has begun to operationalise a more systemic cyber-protection model, ordering MeitY to ensure takedown within 48 hours, develop hash-matching and AI-based detection tools, and block entire rogue websites hosting intimate content. These directions move beyond individual criminal liability to impose technological and regulatory duties on intermediaries, thereby breathing life into due diligence obligations under the IT Act and Rules, and directly addressing the 'hydra-headed' nature of cyber violence against women, where content quickly migrates across platforms and domains.

Parallelly, trial-level jurisprudence on cyberstalking and online harassment, including early cases where men created fake profiles or circulated women's phone numbers and images leading to incessant abuse, has consolidated the use of Sections 469 and 509 IPC together with Section 67 IT Act to secure convictions with custodial sentences, signaling that online misrepresentation, trolling and obscene messaging are not trivial but amount to serious invasions of reputation and sexual autonomy. In a 2025 Mumbai cyberstalking case involving a female celebrity stalked for two years via multiple SIM cards, the court invoked Sections 67 IT Act and Section 78 BNS, leading to swift arrest and underscoring the efficacy of prompt FIRs and telecom data analysis under the new criminal laws. Similarly, in May 2025, the Delhi High Court in a deepfake case against AI-generated obscene content targeting an influencer ordered Meta and X to remove the material, deeming it a privacy violation under Article 21 and reinforcing intermediary accountability for gendered deepfake harms.

MEANING OF CYBERSPACE AND CYBERCRIME

[1] (2015) 5 SCC 1
[2] (2017) 10 SCC 1

'Cyberspace' is a broad phrase. Most of us have a limited understanding of 'Cyberspace' and the crimes that occur in 'Cyberspace,' known as Cybercrime, which occurs on computers and the Internet. Yet, Cybercrime has the potential to have a significant influence on the lives of individuals and our society. As a result, a thorough understanding of Cybercrime is required. Cybercrime is described using a variety of terminology. Previously, it was called 'computer crime,' 'computer-related crime,' or 'crime by computer.' With the spread of digital technology, certain additional words were added to the definition, such as 'high-technology' or 'information-age' crime. In addition, the Internet introduced new terminology such as 'cybercrime' and 'net' crime. Other types of crime include 'digital, electronic, virtual, I.T., high-tech, and technology-enabled.'[3] On the other hand, because there is no inclusion of networks, none of them cover the entire scope of Cybercrime. On the other hand, phrases like high-tech or electronic crime may be too broad to define the crime as specifically Cybercrime because hi-tech breakthroughs occur in other industries as well.[4]

INDIAN LAW ON CYBERCRIME:

- **INFORMATION TECHNOLOGY ACT, 2000**

The exponential growth of digital platforms in India has disproportionately exposed women to cyber-crimes such as online harassment, cyberstalking, identity theft, morphing, revenge pornography, and sexual exploitation. Although the Information Technology Act, 2000 (IT Act) was primarily enacted to provide legal recognition to electronic transactions and facilitate e-governance, its penal provisions have become crucial tools in addressing cyber offences affecting women. The Act on its own and in conjunction with the Indian Penal Code, 1860, is described as the foundation of the jurisprudence of cybercrime in India, especially in protecting the dignity of women, their privacy, and autonomy of their bodies on cyberspace. Section 66E one of the widely discussed provisions concerning women-centric cybercrimes punishes the infringement of privacy through seizure, release or communication of images of intimate aspects of a subject without consent.[5] This section directly targets offences such as voyeurism and non-consensual sharing of intimate images, which predominantly affect women. Similarly, Section 67 criminalises the publication or transmission of obscene material in electronic form, while Section 67A imposes stricter punishment for content containing sexually explicit acts.[6] These provisions are frequently invoked in cases involving online sexual abuse, revenge pornography, and circulation of explicit images of women through social media and messaging platforms. Further, Section 66C and Section 66D deal with identity theft and cheating by personation using computer resources.[7] Women are often targeted through fake social media profiles, impersonation, and fraudulent communication, leading to reputational harm and psychological trauma. Although these sections are gender-neutral in language, their application reveals a gendered impact, with women being more vulnerable due to social stigma and online visibility. The Supreme Court, in *Shreya Singhal v. Union of India*, while striking down Section 66A, emphasised that legitimate restrictions on online abuse must be addressed through narrowly tailored penal provisions rather than vague laws.[8] In addition to punitive measures, the IT Act also casts obligations on intermediaries under Section 79, requiring them to observe due diligence and remove unlawful content upon actual knowledge.[9] This provision is particularly relevant in protecting women from persistent online harassment and abusive content hosted on social media platforms. However, enforcement challenges, lack of cyber literacy, and underreporting by women due to fear of social consequences continue to undermine the effectiveness of these legal safeguards. Therefore, while the IT Act, 2000 provides a statutory framework to combat women-centric cybercrimes, its success depends on robust implementation, gender-sensitive policing, and greater awareness among women regarding their digital rights and remedies.

- **BHARATIYA NYAYA SANHITA (BNS), 2023**

India's reformed legal system, the BNS, has taken steps to combat cybercrimes, enhancing the current IT Act with comprehensive instructions and severe penalties. Section 294 of the BNS addresses obscene content sent electronically, imposing severe penalties for distributing such content online. This action aims to protect public

[3] Nukusheva, Aigul, Roza Zhamiyeva, Viktor Shestak, and Dinara Rustembekova. "Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development." *Security Journal* 35, no. 3 (2022): 893-912.
[4] S. K. Bansal: "Cyber Crimes" (A. P. H. Publishing Corporation, Delhi) 2003.
[5] Information Technology Act, 2000, § 66E.
[6] Information Technology Act, 2000, §§ 67, 67A.
[7] Information Technology Act, 2000, §§ 66C, 66D.
[8] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[9] Information Technology Act, 2000, § 79.

decency and morality by restricting the dissemination of such content and imposing incarceration and fines for repeat offenders.[10]

The Bharatiya Nyaya Sanhita, 2023 significantly strengthens the substantive criminal law framework to address the evolving nature of women-centric cybercrimes, particularly those that exploit digital platforms to cause psychological, sexual, and reputational harm. One of the foundational provisions in this context is *Section 57 – Abetment*, which plays a crucial role in addressing coordinated online abuse. Cyber violence against women is often not an isolated act but a collective phenomenon involving digital mobs, anonymous groups, or organised harassment campaigns. Section 57 enables criminal liability not only for the principal offender but also for individuals or online communities that instigate, encourage, or facilitate such conduct. This is particularly relevant in cases of mass trolling, coordinated reporting, or incitement to threaten or humiliate women on social media, thereby ensuring that indirect perpetrators do not escape accountability.

A central provision dealing directly with gendered digital harm is *Section 69 – Sexual Harassment*, which criminalises unwelcome sexually coloured remarks, demands for sexual favours, and showing pornography against a woman's will. In cyberspace, this provision applies to sexually explicit messages, unsolicited images, obscene comments, and persistent online advances through emails, messaging applications, or social media platforms. By extending the scope of sexual harassment to digital conduct, the BNS acknowledges the reality that virtual spaces can be equally hostile and violating as physical environments. This section strengthens the legal protection earlier provided under IPC Section 354A by aligning it with contemporary modes of communication.

The offence under *Section 70 – Assault or Use of Criminal Force to Woman with Intent to Disrobe*, though traditionally associated with physical acts, acquires renewed relevance in the digital age. Online threats to strip a woman, the creation or circulation of morphed images, and coercion to share intimate photographs through blackmail or extortion constitute serious violations of bodily autonomy and dignity. This provision allows courts to recognise digital acts aimed at sexual humiliation as forms of assault, thereby closing the gap between physical and cyber-enabled violence.

Cyber deception leading to sexual exploitation is addressed under *Section 73 – Sexual Intercourse by Deceitful Means*. This provision is particularly relevant in online romance scams, where women are deceived through fake identities, manipulated profiles, or false promises of marriage, often resulting in sexual exploitation. Complementing this, *Section 74 – Sexual Exploitation of Women* extends protection to cases involving online coercion into producing sexual content, webcam exploitation, and digital trafficking facilitated through online platforms. These sections collectively reflect the BNS's recognition of technology as a tool for exploitation rather than mere communication.

Further, *Section 76 – Sexual Abuse* provides legal recourse against non-penetrative sexual acts facilitated through digital coercion, forced participation in sexual activities online, or cyber-enabled abuse, particularly affecting minors and vulnerable women.

Section 77[11] pertains to voyeurism, a significant violation of privacy. It imposes penalties for those who photograph or disseminate photos of a woman's intimate parts without her permission. This provision mandates severe repercussions for violations, so as to safeguard people's privacy and dignity in the digital era. The BNS emphasises the significance of consent and personal privacy by criminalising such actions.

The BNS prioritises cyber theft significantly. *Section 303* explicitly addresses the larceny of mobile devices, data, or computer hardware and software. It ensures victims will get justice by creating a clear legal framework for prosecuting cyber thieves. This section strengthens the IT Act by fixing loopholes related to digital property theft, making it easier to prosecute and punish such crimes.

Section 78 is crucial in tackling the contemporary offence of cyberstalking. This provision establishes sanctions for both physical and cyber stalking, acknowledging the psychological and emotional damage inflicted by these actions. The BNS seeks to provide a safer online environment by criminalising cyberstalking, especially for at-risk populations like women and children.

[10] Gulshan Shrivastava, et al. "Role of cyber security and cyber forensics in India.". (IGI Global, 2018) pp. 143-161.
[11] BNS, No. 45 of 2023

The BNS also addresses the possession of stolen digital property. *Section 317* imposes penalties on persons possessing stolen mobile phones, computers, or data, regardless of whether they are third parties. This measure diminishes the market for stolen digital products, complicating the ability of hackers to benefit from their unlawful operations.

Some forms of cyber fraud are included under *Section 318*. These include creating fake websites, stealing passwords, and other similar crimes. The severity of the offence determines the punishment, ensuring that it is proportional to the crime. In light of the alarming increase in cases of internet fraud, this provision provides a strong legal barrier to the practice.

Section 336 addresses email spoofing and online forgeries. Those who engage in email spoofing or forgeries with the intent to harm another person's reputation are subject to the penalties outlined in this section. Through the criminalisation of certain conduct, the BNS seeks to protect individuals from reputational damage and ensure the security of online communications.

Psychological intimidation and fear tactics employed online are addressed under *Section 351 – Criminal Intimidation*, which is frequently invoked in cases involving threats of sexual violence, acid attacks, doxxing, or circulation of intimate content. Additionally, *Section 352 – Intentional Insult with Intent to Provoke Breach of Peace* and *Section 356 – Defamation* are crucial in addressing gender-based hate speech, online humiliation, character assassination, and reputational harm suffered by women in digital spaces. Together, these provisions demonstrate that the BNS adopts a comprehensive, dignity-centric approach to combating cybercrimes against women.

- **BHARATIYA NAGARIK SURAKSHA SANHITA, 2023 (BNSS)**

The new BNSS, which replaces the CrPC, is also a considerable reinforcement of the procedural framework of the response against cyber crimes perpetrated against women, especially when it is coupled with the substantive provisions under the Bharatii Nyaya sanhita, 2023 (BNS) and the Information Technology Act, 2000 (IT Act). It stipulates the use of forensic investigations of offences that carry a seven-year or more term of imprisonment in accordance with Section 176(3) BNSS which implies science collecting all digital pieces of evidence such as IP logs, device data, and electronic footprints that could be useful in cases of cyberstalking or online harassment, making it simpler to track down anonymous perpetrators who attack women via social media or email. Such a victim-focused change is apparent in Section 173(1) BNSS, which proposes Zero FIR and e-FIR facilities, where women are now able to report cyber offences directly in real time by digital portals without any jurisdictional ditching, increasing the trauma and delays that might be caused during traditional FIR registration under the old Section 154 CrPC.

Also, and most importantly, BNSS strengthens the handling of evidence under Section 94 and 105, directly allowing prosecutions against crimes such as non-consensual picture passing (BNS Section 77) or cyberstalking (BNS Section 78) by explicitly allowing courts to request electronics like mobiles or laptops to provide access to electronic evidence required by the cyber-investigation, with audio-video recordings of such searches so that evidence retention stays at chain of custody. In section 181 BNSS, the witness statements are modernized and electronic recordings were allowed including video conferencing so that women could be heard although this would reduce re-traumatization and preserve admissibility of digital confessions or victim accounts alongside the IT Act in Sections 66E (violation of privacy) and 67A (explicit content transmission). The 258 BNSS timelines require a ruling within 30-60 days after the arguments, and shorten the trial timeline on cyber offences involving women, where time usually undermines the confidence of victims.

Electronic test trials in the innovations section (BNSS Section 530), update of victim progress (BNSS Section 193) and obligatory forensics (BNS Section 351 read with IT Act Section 66A equivalent) supplement efficacy of the cyber law, preventing programs such as online intimidation (BNS Section 351 read with IT Act Section 66A equivalents) by simplifying the investigation and the subsequent conviction, although issues such as inter-state co-ordination exist. This model will give women power and make the internet a safer environment in India.

- **BHARATIYA SAKSHYA ADHINIYAM, 2023 (BSA)**

The BSA, 2023 supplanting the Indian Evidence Act, 1872, revolutionizes the evidentiary landscape for cybercrimes against women by elevating electronic and digital records to primary evidence status under Section 57, encompassing emails, server logs, WhatsApp chats, GPS data, CCTV footage, and voice messages stored on devices like smartphones or laptops. This parity eliminates the secondary evidence rigmarole of the erstwhile

Section 65B, mandating only a Section 63 certificate from the device custodian or system manager to authenticate records, ensuring admissibility in prosecutions for offences like cyberstalking (BNS Section 78), voyeurism via digital capture (BNS Section 77), or transmission of obscene material (IT Act Section 67A), where screenshots of threats or non-consensual images become directly probative without cumbersome certification hurdles. Section 2(1)(d) BSA expansively defines 'document' to include all digital manifestations, while Section 2(1)(e) integrates electronic statements as oral evidence, fortifying victim testimonies in cases of online harassment or deepfake dissemination, thereby bridging the evidentiary void that previously plagued convictions due to perceived mutability of cyber data.

BSA's victim-centric provisions under Sections 119-136 permit vulnerable women witnesses, including cybercrime survivors, to testify via secure video conferencing from safe locations, often with female officers, mitigating re-traumatization from courtroom confrontations and enhancing participation in trials involving morphed images or persistent digital stalking. Expert opinions on cyber forensics DNA from devices, IP tracing, or hash value verification are bolstered under Sections 45-52 and 113", allowing courts to summon digital specialists to validate blockchain records or encrypted logs, crucial for dismantling anonymity in offences like identity theft (IT Act Section 66C) or privacy breaches targeting women. Presumptions under Sections 61-90 favor authenticity of records from "properly maintained" secure systems, shifting the burden to perpetrators to disprove tampering in revenge porn or slut-shaming cases, while Section 22 safeguards confessions from coercion, ensuring only voluntary electronic admissions hold sway.

This evidentiary empowerment under BSA synergizes with BNS and BNSS, yielding higher conviction rates; for instance, post-2023, digital chain-of-custody protocols have streamlined probes into platform-hosted abuses, deterring gender-based cyber violence amid rising incidents reported by NCRB. However, challenges like cross-border data access and deepfake detection persist, necessitating auxiliary IT Rules amendments for platform compliance. Ultimately, BSA fortifies judicial efficacy, transforming cyber laws into a robust shield for women's digital dignity, privacy, and justice.

DATA ANALYSIS: IMPACT OF CYBER LAWS IN PROTECTION OF WOMEN FROM CYBERCRIMES IN INDIA

1. Trend of Cybercrime Against Women in India (2020–2024)

India has witnessed a **sharp escalation in cybercrime cases**, particularly those affecting women. While the expansion of digital connectivity has empowered women socially and economically, it has also increased their exposure to cyber harassment, identity theft, non-consensual intimate image circulation (NCII), cyberstalking, and online abuse. The enactment of the Information Technology Act, 2000, amendments thereto, and the IT Rules, 2021, aim to provide legal safeguards. However, data suggests that **enforcement capacity and reporting mechanisms remain critical challenges**.

Table 1: Cybercrime Cases in India (Overall) – NCRB Data

Year	Total Cybercrime Cases	% Increase
2019	44,735	—
2020	50,035	+11.8%
2021	52,974	+5.9%
2022	65,893	+24.4%
2023	86,420	+31.2%

Source: NCRB, *Crime in India 2023*

Observation

Cybercrime in India has increased nearly 93% between 2019 and 2023, indicating exponential digital risk exposure. The sharp surge in 2022–23 reflects both increased reporting mechanisms and genuine rise in cyber offences.

Interpretation

While cyber laws exist, the rising trend suggests that legal deterrence remains weak, primarily due to low conviction rates, procedural delays, jurisdictional complexity, and anonymity of offenders. However, the surge also indicates improved reporting access through NCRP and helpline 1930, pointing toward growing victim awareness.

2. Cybercrime Against Women: Scale and Growth (2020–2024)

Gender-disaggregated data reveals a disturbing rise in cyber offences against women.

Table 2: Online Crimes Against Women – NCRP Data

Year	Reported Cases
2020	22,188
2021	28,047
2022	34,349
2023	41,280
2024	48,475

Source: National Cybercrime Reporting Portal (NCRP) Report 2024

Observation

Between 2020 and 2024, online crimes against women increased by 118.4%, highlighting the growing digital vulnerability of women.

Interpretation

This steep rise indicates:

- Increased penetration of smartphones and social media,
- Improved awareness and reporting due to cybercrime portals,
- Yet insufficient preventive and deterrent mechanisms.

Despite strengthened intermediary obligations under IT Rules, 2021, the pace of cybercrime growth suggests that regulatory enforcement is lagging behind technological misuse.

3. Nature of Cybercrimes Affecting Women

Table 3: Major Categories of Cybercrime Against Women (2023)

Type of Offence	Percentage Share
Cyber harassment & bullying	34.2%

Type of Offence	Percentage Share
Sextortion & NCII	27.5%
Cyberstalking	18.6%
Identity theft & impersonation	12.1%
Morphing & deepfake abuse	7.6%

Source: NCRP Annual Analysis Report 2024; Policy Review of Cyber Offences

Observation

Cyber harassment and image-based abuse together account for over 60% of reported offences, indicating that sexualised online violence is the dominant cyber threat against women.

Interpretation

Despite criminalisation under Sections 66E, 67, 67A IT Act and Sections 74–78 BNS, the persistence of these crimes reflects:

- Difficulty in identifying anonymous perpetrators,
- Low platform accountability, and
- Rapid content replication across platforms.

Recent judicial directions mandating hash matching, AI moderation tools, and takedown protocols reflect evolving enforcement but are yet to deliver measurable deterrence.

4. Registration and Charge-Sheeting Efficiency

Table 4: Charge-Sheeting Rate in Cybercrime Against Women Cases

Year	Charge-Sheeting Rate
2020	68.3%
2021	71.6%
2022	74.2%
2023	77.6%

Source: NCRB Crime in India Reports 2020–2023

Observation

Charge-sheeting has improved steadily, indicating greater investigative efficiency.

Interpretation

The upward trend demonstrates institutional strengthening, particularly:

- Expansion of cyber forensic labs,
- Creation of Cyber Crime Cells and I4C infrastructure,
- Judicial insistence on time-bound investigation.

However, conviction rates remain comparatively low, showing that prosecution and evidence management require further strengthening.

5. Regional Distribution of Cybercrimes Against Women (2023)

Table 5: Top States Reporting Cybercrimes

State	Cybercrime Cases
Karnataka	21,889
Telangana	18,236
Maharashtra	14,158
Uttar Pradesh	12,812
Delhi	10,984

Source: NCRB State-wise Cybercrime Data 2023

Observation

Technology hubs report disproportionately high cases, revealing the correlation between digital penetration and cybercrime risk.

Interpretation

Urban, digitally saturated environments create higher vulnerability for women, demanding:

- Localized cyber policing,
- Platform accountability frameworks,
- Gender-sensitive digital safety campaigns.

6. Impact of Cyber Laws on Reporting and Protection

Legal reforms and digital reporting mechanisms have enhanced access to justice.

Table 6: Growth in Cybercrime Reporting via NCRP

Year	Complaints Filed
2020	1.8 million
2021	3.1 million
2022	4.5 million

Year	Complaints Filed
2023	6.9 million

Source: Ministry of Home Affairs, NCRP Data Report

Observation

The nearly fourfold increase reflects growing public trust in cyber law enforcement systems.

Interpretation

Cyber laws, combined with digital reporting infrastructure, have significantly improved victim access, especially for women reluctant to visit police stations due to stigma and fear.

Interpretation and Policy Implications

The data demonstrates that Indian cyber laws have significantly enhanced procedural access, reporting capacity, and institutional responsiveness, but substantive deterrence remains limited. The surge in cybercrime despite legal safeguards reflects:

- Rapid technological expansion,
- Gaps in platform accountability,
- Slow prosecution cycles, and
- Limited victim-centric procedural reforms.

Recent judicial directives mandating automated takedown mechanisms, intermediary liability, and algorithmic monitoring represent a progressive shift. However, for cyber laws to function as effective protective instruments, India must prioritize:

- Specialized cyber courts,
- Mandatory AI moderation protocols,
- Gender-sensitive cyber policing,
- Fast-track NCII takedown systems,
- Nationwide cyber literacy programs.

Thus, while cyber laws have enhanced protection mechanisms, their full deterrent and preventive potential remain partially unrealised, necessitating sustained legal, technological, and institutional reforms.

CONCLUSION

The analysis undertaken in this study demonstrates that India's cyber legal framework has undergone a significant normative and structural evolution in response to the growing menace of cybercrimes against women. Legislative instruments such as the Information Technology Act, 2000, complemented by the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam, 2023, have expanded the scope of criminal liability, procedural efficiency, and evidentiary admissibility in cyberspace. Judicial engagement over the past decade has further constitutionalised cyber harms, recognising online gender-based violence as a violation of women's dignity, equality, and privacy under Article 21. Empirical data from NCRB and NCRP clearly indicates that while cyber offences against women have risen sharply, there has also been a parallel improvement in reporting rates, charge-sheeting, and institutional responsiveness, reflecting increased awareness and

accessibility of cyber justice mechanisms. However, the persistence and scale of cybercrimes reveal that legal reform alone has not translated into adequate deterrence. Enforcement challenges such as anonymity of offenders, cross-border jurisdiction, technological sophistication of crimes, delayed prosecutions, and limited platform accountability continue to undermine the protective potential of cyber laws. Moreover, sociocultural factors including stigma, fear of reputational harm, and digital illiteracy disproportionately affect women's ability to seek timely redress. While recent judicial directions on intermediary obligations, AI-based detection, and rapid takedown mechanisms mark a progressive shift, their impact remains uneven in practice. Indian cyber laws have succeeded in strengthening recognition, access, and procedural protection for women in digital spaces, but their preventive and deterrent effectiveness remains only partially realised. A holistic approach integrating specialised cyber courts, robust forensic infrastructure, gender-sensitive policing, enforceable intermediary liability, and widespread cyber literacy is essential to ensure that cyberspace evolves into a genuinely safe and empowering environment for women.