



# LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.345>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: [www.lijdlr.com](http://www.lijdlr.com)

Under the Platform of LawFoyer – [www.lawfoyer.in](http://www.lawfoyer.in)

---

*After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.*

---

*In case of any suggestions or complaints, kindly contact ([info.lijdlr@gmail.com](mailto:info.lijdlr@gmail.com))*

*To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)*

---

# CYBERCRIME AGAINST WOMEN IN INDIA: A CRITICAL ANALYSIS OF THE LEGAL FRAMEWORK, ENFORCEMENT GAPS AND ACCESS TO JUSTICE

---

Akshita Dixit<sup>1</sup>

## I. ABSTRACT

*The rapid expansion of digital technology has transformed communication, education, employment and social interaction, but it has simultaneously created new spaces for harassment, exploitation and abuse. Women increasingly encounter cyber offences such as cyberstalking, impersonation, identity theft, online harassment, non-consensual dissemination of intimate material, morphing, cyberbullying and other forms of technology-facilitated abuse. The nature of these offences makes them particularly challenging because perpetrators may operate anonymously, evidence can be altered or deleted rapidly, and harmful content can spread across multiple jurisdictions within a short period. This paper examines the Indian legal framework applicable to cybercrime against women and evaluates the extent to which existing laws and institutional mechanisms respond to the distinctive difficulties associated with online offences. It studies relevant provisions of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, together with significant judicial decisions concerning online harassment, privacy, intermediary responsibility and unlawful digital content. The paper further examines institutional mechanisms including the National Cyber Crime Reporting Portal and the Indian Cybercrime Coordination Centre. Particular attention is given to under-reporting, difficulties in identification of perpetrators, preservation and admissibility of electronic evidence, intermediary cooperation, privacy concerns and the emotional and social consequences experienced by victims. The study adopts a doctrinal methodology supported by secondary literature and government materials. It argues that although India possesses several overlapping legal remedies, the framework remains fragmented and its*

---

<sup>1</sup> 1st-Semester B.A. LL.B. (Hons.) Student at The Maharaja Sayajirao University of Baroda, Gujarat (India).  
Email: [akshitadixit3164@gmail.com](mailto:akshitadixit3164@gmail.com)

*effectiveness depends substantially upon implementation, technological capacity and victim-oriented reporting mechanisms. The paper proposes measures aimed at improving investigation, digital evidence handling, institutional coordination, awareness and access to justice.*

## **II. KEYWORDS**

Cybercrime, Women, Cyberstalking, Online Harassment, Cyber Law.

## **III. INTRODUCTION AND RESEARCH PROBLEM**

The internet has become an essential part of contemporary life. Communication, education, banking, employment, entertainment and social relationships increasingly operate through digital platforms. This expansion has provided individuals with unprecedented opportunities to participate in public and private life. At the same time, the digital environment has become a site in which existing forms of discrimination and violence can be reproduced and new forms of abuse can emerge.

Cybercrime against women cannot be understood merely as conventional crime transferred from the physical world to the internet. Digital technology can increase the speed, reach and persistence of harmful conduct. A threatening message can be sent repeatedly without physical proximity; an intimate image can be copied and redistributed to an unknown number of people; a fake account can be created using another person's identity; and personal information can be collected from different online sources and used to harass or intimidate a victim.

The literature supplied for this study identifies cyberstalking, cyber harassment, cyber defamation, morphing, cyber pornography, hacking, trolling, cyberbullying and identity-related offences among the forms of gender-based violence that may occur online. Another study specifically examining cybercrime against women discusses stalking, ransomware, defamation, bullying, pornography and cyber grooming as significant forms of online abuse.

The problem, however, is not simply the existence of these offences. The more significant legal question concerns the ability of the legal system to respond effectively after an

offence has occurred. A victim may know that the conduct is unlawful but may not know which authority to approach, what evidence to preserve, which statutory provision applies or how to obtain removal of harmful content. The perpetrator may use anonymous accounts, false identities, multiple devices or platforms located in different jurisdictions. Consequently, the gap between the existence of a legal remedy and the accessibility of that remedy becomes central to the question of access to justice.

India does not presently address every form of technology-facilitated gender-based violence through one consolidated statute. Instead, applicable remedies are distributed across the Information Technology Act, 2000, general criminal law, data protection legislation and procedural and evidentiary rules. The earlier literature similarly observed that there is no single legislation specifically dedicated to gender-based violence in cyberspace and that different statutes operate together.

The legal landscape has also changed significantly since some of the earlier literature was published. The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code, 1860 as the principal penal statute from 1 July 2024. Consequently, contemporary analysis must examine the present statutory framework rather than relying exclusively upon the IPC provisions frequently cited in earlier research.

The research problem addressed in this paper is therefore:

*Whether the existing Indian legal framework, despite providing multiple remedies against cybercrime affecting women, is sufficiently comprehensive and effectively implemented to ensure prevention, investigation, victim protection and access to justice.*

### **A. Research Objectives**

The research has the following objectives:

1. To examine the major forms of cybercrime and technology-facilitated abuse affecting women in India.

2. To analyse the statutory framework governing cyber offences against women, particularly under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023.
3. To examine the role of privacy and data protection law in protecting women from misuse of personal information in cyberspace.
4. To analyse significant judicial decisions that have contributed to the development of Indian cyber jurisprudence.
5. To identify practical and institutional challenges in reporting, investigating and prosecuting cyber offences.
6. To examine existing governmental mechanisms for reporting and addressing cybercrime.
7. To suggest legal and institutional measures for improving access to justice for victims.

## **B. Research Questions**

The paper seeks to answer the following questions:

1. What are the principal forms of cybercrime affecting women in India?
2. What legal remedies are presently available to women who experience cybercrime?
3. How effectively do the Information Technology Act, 2000 and Bharatiya Nyaya Sanhita, 2023 address technology-facilitated offences against women?
4. What role can privacy and data protection law play in preventing and responding to online abuse?
5. What are the principal barriers to reporting, investigation and prosecution of cybercrime against women?
6. How have Indian courts contributed to the development of legal protection against online abuse?
7. What reforms can improve access to justice and victim protection?

### **C. Research Hypothesis**

The existing Indian legal framework provides multiple statutory remedies for cybercrime against women, but its effectiveness is constrained by fragmentation of legal remedies, difficulties in attribution and digital evidence, insufficient technological capacity, under-reporting and limited awareness among victims. Strengthening institutional coordination, evidence-handling capabilities and victim-oriented reporting mechanisms can significantly improve access to justice.

### **D. Research Methodology**

The research primarily adopts a doctrinal legal research methodology. Primary sources include legislation and judicial decisions relevant to cybercrime, privacy, online harassment and digital evidence. The principal statutory materials examined include the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023.

Secondary sources include academic literature, research papers, institutional publications and government materials. The two studies used as background literature provide useful discussions of the forms of cybercrime, legal provisions, judicial decisions, government initiatives and reporting difficulties. The LIJDLR study additionally contains empirical survey findings concerning awareness and reporting behaviour among cyber users.

The present paper does not treat that survey as original empirical research. Instead, its findings are used as secondary literature to identify issues requiring further doctrinal examination.

The research is analytical rather than statistical. The paper examines the relationship between statutory protection and practical access to justice, with particular attention to the difficulties arising from the technological nature of cyber offences.

## E. Literature Review

Existing literature demonstrates that cybercrime affecting women takes several forms and cannot be restricted to financial fraud. Jyoti's study, *Cyber Crimes Against Women in India*, identifies cyberstalking, ransomware, cyber defamation, cyberbullying, cyber pornography and cyber grooming among the forms of cybercrime relevant to women. It also discusses statutory provisions and preventive measures.

Kanakshi Nema's article, *Gender Based Violence in Cyberspace: A Critical Analysis of Legal Framework in India*, takes a broader gender-based-violence approach. It discusses cyberstalking, cyber harassment, cyber defamation, morphing, cyber pornography, hacking, trolling and cyberbullying, while examining the Information Technology Act and provisions of the then-applicable IPC. The study further considers judicial decisions and government initiatives and identifies problems relating to anonymity, intermediary obligations, electronic evidence and reporting.

The literature also indicates that under-reporting is a significant problem. The survey contained in Nema's study recorded concerns including social stigma, lack of family support, fear of social judgment, perceived ineffectiveness of authorities and the time and cost associated with reporting.

However, an important limitation in earlier literature is the changing legal framework. Several studies continue to organise the analysis primarily around the IPC provisions that were applicable before the commencement of the BNS. The present study therefore seeks to update the legal analysis by examining the post-2024 criminal law framework and considering how it operates alongside the Information Technology Act and emerging data-protection law.

The research gap is consequently located at the intersection of women-specific criminal protection, technology-specific legislation, privacy, enforcement and access to justice under India's current legal framework.

## **IV. UNDERSTANDING CYBERCRIME AGAINST WOMEN**

### **1. Cyberstalking**

Cyberstalking involves the repeated use of electronic communication or digital technology to monitor, contact, threaten or harass an individual. The digital environment can make stalking persistent because communication can continue through multiple accounts and platforms.

The earlier literature identifies practices such as monitoring social-media activity, tracking locations through digital tools, impersonation and repeated unwanted communication as forms of cyberstalking.

Cyberstalking may be particularly intrusive because the perpetrator does not necessarily need physical access to the victim. Information voluntarily shared on social media can be combined with other publicly available information to construct a detailed picture of a person's movements, relationships and activities.

### **2. Online Harassment and Cyberbullying**

Online harassment can involve repeated threatening, abusive, sexually explicit or humiliating communication. Cyberbullying may involve the publication or circulation of degrading or hostile content through social-media platforms.

Unlike a private conversation, online harassment may become visible to a large audience. The persistence of digital content can also increase the duration of harm even after the original communication has ended.

### **3. Impersonation and Identity Theft**

Digital identities can be misused through fake social-media profiles, fraudulent email accounts, stolen passwords or unauthorised access to accounts. The perpetrator may use the victim's photograph, name or other personal information to communicate with third parties.

Such conduct may cause reputational harm while simultaneously making it difficult for the victim to establish that the account or communication was not genuinely hers.

#### **4. Morphing and Non-Consensual Intimate Content**

Technological tools make it increasingly easy to manipulate photographs and videos. Morphing involves altering or combining images so that an individual's face or identity appears in another context. When such manipulated material is sexualised and circulated without consent, the resulting harm may include humiliation, blackmail, reputational injury and threats.

The literature identifies morphing and the non-consensual circulation of intimate material as important forms of online gender-based abuse.

#### **5. Cyber Defamation**

Defamatory statements can spread rapidly through digital platforms. The online environment can increase the audience exposed to allegedly defamatory material and make reproduction easier.

At the same time, cyber defamation must be distinguished from every form of offensive or abusive communication. Whether particular conduct constitutes defamation depends upon the applicable legal elements, including the nature of the statement, publication, reputational harm and available statutory exceptions.

### **V. INDIAN LEGAL FRAMEWORK**

#### **A. Information Technology Act, 2000**

The Information Technology Act remains the principal legislation specifically dealing with computer-related offences.

- 1. Section 66C: Identity Theft:** Section 66C addresses fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. This provision can become relevant when a perpetrator

obtains access to a woman's digital account or credentials and uses them without authorisation.

2. **Section 66D: Cheating by Personation:** Section 66D addresses cheating by personation through communication devices or computer resources. It is relevant to digital impersonation and fraudulent representations made through online systems.
3. **Section 66E: Violation of Privacy:** Section 66E addresses intentional or knowing capture, publication or transmission of an image of a private area of a person without consent, subject to the statutory requirements. This provision has particular relevance to cases involving non-consensual intimate imagery.
4. **Sections 67 and 67A:** Section 67 addresses publication or transmission of obscene material in electronic form, while Section 67A addresses material containing sexually explicit acts or conduct.

These provisions may become relevant where sexually explicit or obscene material is created, published or transmitted electronically. The statutory scheme therefore provides criminal remedies even where the conduct is not captured by a single women-specific offence.

The Information Technology Act itself contains these specific offences, including identity theft, cheating by personation, violation of privacy and electronic publication of obscene or sexually explicit material.

## **B. Bharatiya Nyaya Sanhita, 2023**

A contemporary study of cybercrime against women must account for the transition from the Indian Penal Code to the Bharatiya Nyaya Sanhita.

1. **Sexual Harassment – Section 75:** Section 75 of the BNS covers sexual harassment and includes, among other conduct, showing pornography against the will of a woman and making sexually colored remarks. Where such conduct

occurs through digital communication, the provision may operate alongside the Information Technology Act depending upon the facts of the case.

2. **Voyeurism – Section 77:** Section 77 addresses voyeurism, including watching, capturing or disseminating the image of a woman engaged in a private act in circumstances where she would ordinarily expect privacy. The provision is particularly significant in the context of digitally recorded private material.
3. **Stalking – Section 78:** The BNS retains a specific offence of stalking. The offence encompasses repeated following or contacting of a woman despite a clear indication of disinterest and also includes monitoring the use by a woman of the internet, email or another form of electronic communication. The inclusion of electronic monitoring within the stalking provision recognises that stalking can occur without physical proximity.
4. **Words, Gestures and Acts Intended to Insult the Modesty of a Woman:** The BNS also retains protection against specified words, gestures or acts directed at a woman with the requisite intention concerning her modesty. Depending upon the factual circumstances, digitally transmitted communications may form part of conduct attracting criminal liability.
5. **Defamation:** The BNS separately provides for defamation. Online publication does not create a completely separate law of defamation; rather, the ordinary elements of the offence must be applied to communication through digital platforms.

The coexistence of general criminal provisions with the IT Act demonstrates the fragmented nature of the present legal framework: one incident may potentially engage several statutory provisions depending upon the exact conduct involved.

### C. Privacy and Data Protection

Cybercrime against women frequently involves misuse of personal information. Telephone numbers, photographs, location information, account credentials, private

conversations and other personal data may be collected or misused in the course of online abuse.

The Supreme Court's recognition of privacy as a constitutionally protected right in *Justice K.S. Puttaswamy (Retd.) v Union of India* provides an important constitutional foundation for understanding informational privacy.

The Digital Personal Data Protection Act, 2023 establishes a statutory framework for processing digital personal data. India Code describes the Act as legislation concerning the processing of digital personal data while recognising an individual's interest in protecting personal data.

However, data protection and criminal law serve different functions. Data protection regulation is principally concerned with lawful processing and protection of personal data, whereas criminal law addresses conduct that constitutes an offence. Therefore, the existence of data protection legislation does not eliminate the need for criminal remedies against stalking, impersonation, threats, intimate-image abuse or other forms of digital violence.

The implementation position must also be carefully considered. The Central Government's commencement notification provides for different provisions of the DPDP Act to come into force on different dates, meaning that the statutory framework should not be described as if every provision has operated from the date of enactment.

## VI. JUDICIAL DEVELOPMENT

### A. *Suhas Katti v State of Tamil Nadu*

*Suhas Katti* is widely recognised in Indian cyber-law literature as an important early conviction involving obscene online material and harassment. The case concerned the use of a fake email account and publication of objectionable material following the accused's failed relationship with the victim. The case demonstrated that existing criminal provisions and the IT Act could be applied to conduct occurring through electronic communication.

The importance of the case lies not merely in the conviction but in demonstrating that digital conduct can produce legally recognisable harm and can be investigated through specialised cybercrime mechanisms.

### **B. Shreya Singhal v Union of India**

In *Shreya Singhal v Union of India*, the Supreme Court struck down Section 66A of the Information Technology Act for violating the constitutional guarantee of freedom of speech and expression.

The decision is important because cybercrime regulation cannot operate without constitutional limits. The State's legitimate interest in preventing online abuse must coexist with the protection of lawful expression.

The case therefore demonstrates that stronger regulation does not automatically mean broader criminalisation. Legal rules must satisfy constitutional standards of clarity and proportionality.

### **C. Avnish Bajaj v State**

The *Avnish Bajaj* litigation raised questions concerning intermediary responsibility in relation to unlawful online material. The case contributed to the development of Indian discussion regarding intermediary liability and the responsibility of platforms operating in the digital environment. The literature examined for this paper identifies the case as part of the evolving judicial approach to online sexual material.

Its relevance continues because contemporary online abuse often depends upon platforms through which content is uploaded, stored, shared or redistributed.

### **D. Justice K.S. Puttaswamy (Retd.) v Union of India**

The constitutional recognition of privacy is particularly relevant to cybercrime against women because many such offences involve unauthorised access to personal accounts, surveillance, disclosure of intimate information or misuse of personal data.

Privacy in the digital environment cannot be reduced to physical secrecy. Control over personal information, autonomy and dignity are also significant dimensions of the right to privacy.

## **VII. INSTITUTIONAL MECHANISMS AND ACCESS TO JUSTICE**

### **1. National Cyber Crime Reporting Portal**

The National Cyber Crime Reporting Portal provides an online mechanism through which victims can report cybercrime. The official portal specifically provides reporting options for women and children-related cybercrime, including an option to report anonymously in relevant categories.

The portal also provides facilities for reporting financial fraud and other cybercrime. The official system states that complaints are dealt with by law-enforcement agencies based on the information submitted.

The availability of an online reporting mechanism is important because victims may hesitate to approach a physical police station, particularly where the offence concerns intimate material, sexual harassment or reputational harm.

### **2. Cyber Crime Helpline**

The national cybercrime system identifies 1930 as the cybercrime helpline, particularly important for immediate reporting of cyber financial fraud.

Awareness of such mechanisms is nevertheless essential. A reporting system can only improve access to justice when victims know that it exists and understand how to use it.

### **3. Indian Cybercrime Coordination Centre**

The Indian Cybercrime Coordination Centre, or I4C, represents an institutional approach to improving coordination in cybercrime investigation and response. The literature examined for this research identifies I4C as part of India's broader institutional response to cybercrime and digital forensics.

## VIII. MAJOR ENFORCEMENT GAPS

1. **Fragmentation of Legal Remedies:** The first difficulty is fragmentation. A single incident may simultaneously involve stalking, identity theft, privacy violations, obscene material, intimidation and defamation. There may therefore be no single provision that completely describes the harm experienced by the victim. Multiple statutes may need to be applied together. This can create complexity for both victims and investigating authorities.
2. **Identification of Anonymous Perpetrators:** Anonymity and pseudonymity remain important challenges in cyber investigations. A perpetrator may create multiple accounts, use false identities or operate through technological infrastructure that complicates attribution. The earlier LIJDLR study similarly identifies anonymity as a major challenge in cyberspace and calls for stronger mechanisms for identification and tracking of perpetrators.
3. **Preservation of Electronic Evidence:** Digital evidence is inherently vulnerable to alteration, deletion and loss. Screenshots may establish that particular content was visible, but investigators may require additional information concerning the account, device, metadata, source and chain of custody. The effectiveness of cybercrime prosecution therefore depends not merely on the existence of offences but also on the ability of investigating agencies to collect and preserve technically reliable evidence.
4. **Intermediary Cooperation:** Digital platforms often possess information relevant to identifying users and tracing activity. At the same time, intermediary obligations must be balanced with privacy, free expression and due-process considerations. The earlier literature identifies the role of intermediaries as an important unresolved issue in combating gender-based violence online.
5. **Under-Reporting:** Under-reporting remains a serious obstacle because cybercrime may involve shame, fear of social judgment, family pressure or concern that reporting itself will expose private material. The survey reviewed in the LIJDLR

article found that respondents identified stigma, lack of family support, fear of social judgment, perceived ineffectiveness of authorities and reporting costs among the reasons for reluctance to report.

These findings should not automatically be treated as nationally representative because the survey involved 115 cyber users. Nevertheless, they illustrate the kinds of barriers that may prevent victims from entering the formal justice system.

## **IX. IMPACT ON VICTIMS**

The consequences of cybercrime against women are not restricted to the immediate digital event.

A manipulated photograph, threatening message or fake profile may affect a victim's reputation, relationships, education, employment and participation in social media. Persistent online harassment may also result in withdrawal from digital spaces.

The literature reviewed for this study records instances where victims reported emotional consequences, withdrawal from social media and fear arising from cyberstalking or non-consensual sharing of intimate content.

The legal system should therefore recognise that the harm produced by cybercrime may continue after the original content is removed. Victim support cannot be limited to prosecution of the offender. It should also include mechanisms for assistance, privacy protection, content removal where legally appropriate and psychological support.

## **X. CRITICAL ANALYSIS**

The Indian legal framework cannot fairly be characterised as completely lacking remedies for cybercrime against women. The Information Technology Act provides technology-specific offences; the BNS contains gender-specific offences that may apply to digital conduct; constitutional jurisprudence protects privacy; and the Government has established online reporting mechanisms.

The more difficult issue is whether these components operate together effectively:

1. First, the framework is distributed across multiple legal regimes. This provides flexibility but may also produce uncertainty for victims who are unfamiliar with the law.
2. Second, the law cannot remain effective merely by creating additional offences. Cybercrime is technologically dynamic. An offence involving one platform today may be committed through a completely different technological environment tomorrow.
3. Third, investigation capacity is crucial. A well-drafted provision has limited practical value if law-enforcement personnel lack the technical expertise necessary to identify perpetrators or preserve electronic evidence.
4. Fourth, victim confidence is central to access to justice. The availability of an online portal is an important step, but reporting mechanisms should be simple, confidential and responsive.
5. Fifth, regulation must respect constitutional rights. The experience of Section 66A demonstrates the danger of vague criminal provisions. Measures directed at harmful online conduct must be sufficiently precise so that legitimate expression is not unnecessarily criminalised.

The objective should therefore not be unrestricted expansion of criminal law. The more sustainable approach is a combination of precise offences, effective investigation, platform cooperation, digital literacy, victim support and constitutional safeguards.

## **XI. SUGGESTIONS AND RECOMMENDATIONS**

1. **Evaluate the Effectiveness of the Emerging Regulatory Framework:** India should evaluate the practical adequacy and enforcement of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, particularly compliance with SGI labelling and provenance requirements and the two-hour complaint-based and three-hour actual-knowledge removal timelines. Particular attention should be given to the effective regulation of non-

consensual intimate deepfakes, including 'nudifying' tools, alongside evolving judicial interpretation of intermediary takedown obligations

2. **Strengthen Cybercrime Investigation Units:** Police personnel dealing with cybercrime should receive regular training in digital forensics, account attribution, preservation of electronic evidence, platform procedures and privacy-sensitive investigation. Specialised training should also cover the particular vulnerabilities associated with gender-based cybercrime.
3. **Improve Evidence Preservation:** Standardised protocols should be developed for victims and investigators regarding preservation of screenshots, URLs, account information, metadata and other relevant digital material. Victims should be advised not to delete threatening messages or other evidence before reporting, where preservation is safe and feasible.
4. **Make Reporting Mechanisms Victim-Centred:** The National Cyber Crime Reporting Portal should remain accessible and easy to navigate. Reporting procedures concerning sexual or intimate material should minimise unnecessary disclosure of the victim's identity. The availability of anonymous reporting in appropriate categories is a useful mechanism, but victims should also receive clear information about what happens after a complaint is submitted.
5. **Improve Intermediary Coordination:** Social-media platforms and other intermediaries should maintain clear mechanisms for responding to lawful requests from investigating agencies and for dealing with unlawful content. At the same time, intermediary obligations should remain consistent with constitutional rights and procedural safeguards.
6. **Increase Digital and Legal Literacy:** Awareness campaigns should not merely instruct women to "be careful online." Such messaging can unintentionally shift responsibility from perpetrators to victims. Cyber-safety education should instead explain:
  - how to identify suspicious communications;
  - how to secure accounts;

- how to preserve evidence;
  - how to report cybercrime;
  - available legal remedies;
  - privacy settings;
  - risks associated with sharing sensitive information; and
  - available victim-support mechanisms.
7. **Strengthen Victim Support:** Victims should have access to legal assistance and psychological support, particularly in cases involving sexual harassment, intimate-image abuse, blackmail or persistent stalking.
8. **Encourage Platform-Level Safety Measures:** Platforms should improve mechanisms for reporting impersonation, harassment and non-consensual intimate material. Repeat offenders and coordinated harassment should receive appropriate attention within platform governance systems.
9. **Promote Gender-Inclusive Protection:** Although women experience significant forms of gender-based cyber violence, online abuse is not exclusively experienced by women. Legal protection should therefore address gender-based harm without denying protection to male or gender-diverse victims.

## XII. CONCLUSION

The digital transformation of Indian society has created significant benefits, but it has also expanded the environment in which harassment, surveillance, impersonation, privacy violations and gender-based abuse can occur. Women may experience cybercrime through stalking, harassment, impersonation, identity theft, morphing, non-consensual intimate imagery, cyberbullying and related forms of digital abuse.

India possesses several legal and institutional mechanisms capable of addressing these forms of conduct. The Information Technology Act provides technology-specific offences, while the Bharatiya Nyaya Sanhita contains provisions relating to sexual harassment, voyeurism, stalking and other offences that may apply to conduct occurring through electronic communication. Privacy jurisprudence and the developing data-

protection framework provide additional legal dimensions. The National Cyber Crime Reporting Portal provides a direct mechanism for reporting cyber offences and gives special attention to women and children.

However, the existence of legal provisions does not automatically ensure access to justice. The principal challenges lie in the fragmentation of remedies, technological anonymity, difficulties in collecting and preserving electronic evidence, intermediary cooperation, limited awareness and under-reporting. The research examined also identifies social stigma and lack of confidence in reporting mechanisms as important barriers.

The central issue is therefore not simply whether India has laws governing cybercrime against women. It is whether those laws can be translated into accessible and effective remedies for victims.

A meaningful response requires coordination between legislation, law enforcement, courts, technology platforms, educational institutions and civil society. Legal reform should be accompanied by technical training, evidence-preservation mechanisms, confidential reporting procedures, digital literacy and victim support.

Cybersecurity should consequently be understood not merely as a technical concern but also as an issue of dignity, privacy, equality and access to justice. A safer digital environment will depend upon ensuring that technological progress is accompanied by legal accountability and effective protection of individuals who experience abuse online.

### **XIII. REFERENCES**

#### **A. Primary Sources**

1. The Information Technology Act, 2000.
2. The Bharatiya Nyaya Sanhita, 2023.
3. The Digital Personal Data Protection Act, 2023.
4. The Constitution of India.
5. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended by the Information Technology

(Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), dated 10 February 2026 (w.e.f. 20 February 2026), as corrected by G.S.R. 148(E), dated 26 February 2026.

6. *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.
7. *Shreya Singhal v Union of India*, (2015) 5 SCC 1.
8. *Suhas Katti v State of Tamil Nadu*, C.C. No. 4680 of 2004.
9. *Avnish Bajaj v State*, 150 DLT 769 (2008).

## B. Secondary Sources

1. Jyoti, *Cyber Crimes Against Women in India*, SSRN Electronic Journal.
2. Kanakshi Nema, "Gender Based Violence in Cyberspace: A Critical Analysis of Legal Framework in India," *LawFoyer International Journal of Doctrinal Legal Research*, Vol. I, Issue IV (2024).
3. Association for Progressive Communications, *Voices from Digital Spaces: Technology-Related Violence Against Women* (2011).
4. United Nations Broadband Commission Working Group on Broadband and Gender, *Cyber Violence Against Women and Girls: A Worldwide Wake-Up Call* (2015).
5. Government of India, Ministry of Home Affairs, Indian Cybercrime Coordination Centre.
6. National Cyber Crime Reporting Portal, Government of India.
7. National Commission for Women, Government of India.
8. National Crime Records Bureau, *Crime in India* reports.
9. Observer Research Foundation, publications concerning gender-based violence in private online spaces.
10. Dr. Nuzhat Parveen Khan, *Women and the Law*.