
CYBER CRIME AGAINST WOMEN IN INDIA: THE GAP BETWEEN LEGAL PROTECTION AND EFFECTIVE ENFORCEMENT

M. Vanitha, B.Com (CA), LL.B., S. Thangapazham Law College, Vasudevanallur, Tenkasi, Tamilnadu.

K. Rajesh Kumar, B.Com. ML., (Ph.D), Faculty of Law, S. Thangapazham Law College, Vasudevanallur, Tenkasi, Tamilnadu.

1. ABSTRACT

Cybercrime against women has emerged as one of the most pressing challenges in India's digital era. The rapid growth of internet usage, social media platforms, and digital communication has significantly increased opportunities for cyber offenders to target women through cyberstalking, online harassment, identity theft, cyberbullying, revenge pornography, sextortion, online defamation, and financial fraud. Although India has established a legal framework through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and various provisions relating to electronic evidence and cyber offences, the effectiveness of these laws remains limited due to gaps in enforcement. Delayed investigations, inadequate cyber forensic infrastructure, lack of trained personnel, jurisdictional challenges, underreporting of offences, and low public awareness continue to hinder the delivery of justice.

This study critically examines the gap between legal protection and effective enforcement in addressing cybercrime against women in India. It analyses the existing legislative framework, the role of law enforcement agencies, judicial responses, and institutional mechanisms for victim protection. The research further explores the socio-cultural factors that discourage women from reporting cybercrimes, including fear of social stigma, victim blaming, privacy concerns, and lack of confidence in the criminal justice system. By reviewing recent legal developments, judicial decisions, government initiatives, and empirical studies, the paper identifies key weaknesses in the current enforcement process and evaluates their impact on victims' access to justice.

The study concludes that while India possesses a reasonably comprehensive legal framework to combat cybercrime against women, the primary challenge lies in its effective implementation. Strengthening cyber policing, improving digital forensic capabilities, enhancing inter-agency coordination,

promoting legal awareness, encouraging timely reporting, and adopting victim-centred approaches are essential to bridge the gap between law and enforcement. A holistic strategy integrating legal reforms, technological advancements, institutional capacity building, and public awareness is necessary to ensure meaningful protection of women's digital rights and online safety in India.

2. Keywords: Cyber Crime, Women, Cyber Stalking, Online Harassment, Cyber Sexual Abuse, Information Technology Act, Bharatiya Nyaya Sanhita, Digital Evidence, Privacy, Cyber Security.

3. Introduction

The rapid expansion of information and communication technology has transformed the way individuals communicate, conduct business, access education, and participate in social life. In India, increasing internet penetration, affordable smartphones, and widespread use of social media platforms have created unprecedented opportunities for digital connectivity. However, these technological advancements have also resulted in a significant rise in cybercrimes, particularly those targeting women. The digital environment has become a space where women are increasingly exposed to various forms of online abuse, including cyberstalking, cyberbullying, identity theft, online impersonation, non-consensual sharing of intimate images, revenge pornography, sextortion, online defamation, and financial fraud.

Cybercrime against women is not merely a technological issue but also a serious violation of human rights, privacy, dignity, and personal security. The psychological, emotional, social, and economic consequences of such offences can be severe, often leading to anxiety, depression, reputational damage, loss of employment opportunities, and withdrawal from digital platforms. Many victims hesitate to report these crimes due to fear of social stigma, victim blaming, concerns about privacy, and lack of confidence in the criminal justice system. Consequently, a substantial number of cybercrimes remain unreported, making the problem more pervasive and difficult to address.

India has enacted several legal measures to combat cybercrime, including the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, which contain provisions addressing electronic offences, online harassment, identity theft, and other cyber-related crimes. The government has also established specialised cybercrime police stations, cyber forensic laboratories, online complaint portals, and awareness programmes to strengthen

cybersecurity and victim assistance. Despite these developments, enforcement continues to face numerous challenges, including inadequate technical infrastructure, shortage of trained cybercrime investigators, jurisdictional complexities, delays in investigation and prosecution, and limited coordination among law enforcement agencies.

The gap between legal protection and effective enforcement has become one of the most significant obstacles in ensuring justice for women affected by cybercrime. While the legislative framework provides legal remedies, practical implementation often falls short due to institutional weaknesses and procedural delays. This gap undermines public confidence in the justice system and reduces the deterrent effect of cybercrime laws.

This research critically examines the existing legal framework governing cybercrime against women in India and evaluates the effectiveness of its enforcement mechanisms. It analyses the causes of enforcement failures, identifies the challenges faced by victims and investigating agencies, and assesses recent legal and policy developments. The study also explores measures to strengthen cyber policing, improve digital forensic capabilities, enhance legal awareness, and promote a victim-centred approach to justice. By bridging the gap between legal protection and practical enforcement, India can create a safer digital environment that upholds women's rights, protects their dignity, and ensures equal access to justice in the digital age.

4. STATEMENT OF THE PROBLEM

The increasing use of the internet, social media and digital communication platforms has created new forms of vulnerability for women in India. Cyber crimes such as cyber stalking, online harassment, cyber bullying, identity theft, impersonation, cyber sexual harassment, cyber defamation and the non-consensual sharing of intimate images are becoming significant threats to the privacy, dignity and security of women. Although India has enacted several legal provisions to address cyber-related offences, the existence of laws alone has not ensured effective protection for victims.

A major problem lies in the gap between the legal protection available on paper and its effective implementation in practice. Victims often face difficulties in reporting cyber offences, identifying offenders, preserving digital evidence and obtaining timely remedies. Anonymity in cyberspace, rapidly changing technology, lack of adequate technical expertise, limited institutional capacity, delays in investigation and prosecution, and insufficient awareness

among victims further complicate the enforcement process. Under-reporting of cyber crimes due to fear of social stigma, privacy concerns and lack of confidence in the justice system also remains a serious concern.

Therefore, the central problem addressed by this study is whether the existing legal and institutional mechanisms in India are sufficiently effective in preventing, investigating and providing remedies for cyber crimes against women. The study seeks to identify the gaps between statutory protection and actual enforcement and to examine whether the existing framework adequately safeguards the privacy, dignity and safety of women in the digital environment.

5. Review of Literature

A review of existing literature reveals that cybercrime against women has become an important area of legal and socio-technological research in India. Scholars have examined the increasing prevalence of online offences, the adequacy of legal safeguards, challenges in law enforcement, and the need for stronger institutional mechanisms. The following studies provide valuable insights into the existing body of knowledge.

5.1. Aparna Viswanathan (2012) – Cyber Law: Indian and International Perspectives

Aparna Viswanathan examined the evolution of cyber law in India and analysed the effectiveness of the Information Technology Act, 2000, in addressing emerging cyber offences. The author argued that although the legal framework provides statutory protection against cybercrime, rapid technological developments often outpace legal reforms. The study highlighted the need for regular legislative updates, specialised investigation mechanisms, and judicial capacity-building to ensure effective implementation of cyber laws.

5.2. Pavan Duggal (2017) – Cyberlaw: The Indian Perspective

Pavan Duggal discussed India's cyber legal framework and emphasised that cybercrime has become increasingly sophisticated with technological advancements. The study observed that women are particularly vulnerable to offences such as cyberstalking, online harassment, identity theft, and revenge pornography. The author stressed that the major challenge lies not in the absence of laws but in weak enforcement, limited cyber forensic capabilities, and inadequate awareness among law enforcement agencies and the public.

5.3. Debarati Halder and K. Jaishankar (2011) – Research on Cybercrime Against Women

Halder and Jaishankar explored gender-based cyber victimisation and examined the psychological and social consequences of online abuse against women. Their research found that many victims hesitate to report cybercrimes due to fear of social stigma, privacy concerns, victim blaming, and lack of confidence in the criminal justice system. The study recommended victim-sensitive policing, awareness programmes, and stronger legal enforcement to encourage reporting and improve access to justice.

5.4. Ministry of Home Affairs, Government of India (National Cyber Crime Reporting Portal Reports)

Reports issued by the Ministry of Home Affairs indicate a steady increase in cybercrime complaints involving women, including cyberstalking, online impersonation, financial fraud, and circulation of intimate images without consent. The reports highlight government initiatives such as the National Cyber Crime Reporting Portal, specialised cybercrime police stations, and cyber awareness campaigns. However, they also acknowledge persistent challenges relating to delayed investigations, shortage of trained personnel, and technological limitations in cybercrime enforcement.

5.5. National Crime Records Bureau (NCRB) – Crime in India Reports

The NCRB's annual *Crime in India* reports provide statistical evidence of the increasing number of cybercrime cases across the country. The reports demonstrate that women continue to be disproportionately affected by cyber harassment, identity theft, and online exploitation. Despite the growing number of registered cases, conviction rates remain comparatively low, indicating significant gaps in investigation, evidence collection, and prosecution. The reports reinforce the need to strengthen institutional capacity and improve coordination among law enforcement agencies.

6. Research Objectives

The present study, titled “**Cybercrime Against Women in India: The Gap Between Legal Protection and Effective Enforcement,**” aims to critically examine the effectiveness of India's legal and institutional framework in addressing cybercrimes against women. The

specific objectives of the study are as follows:

1. **To examine the nature and extent of cybercrime against women in India**, including offences such as cyberstalking, cyberbullying, online harassment, identity theft, sextortion, revenge pornography, online impersonation, and financial cyber fraud.
2. **To analyse the existing legal framework governing cybercrime against women in India**, with particular reference to the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and other relevant laws and regulations.
3. **To evaluate the effectiveness of law enforcement agencies and the criminal justice system** in investigating, prosecuting, and preventing cybercrimes against women.
4. **To identify the major challenges and gaps in the enforcement of cyber laws**, including issues relating to digital evidence, cyber forensic infrastructure, jurisdictional complexities, shortage of trained personnel, delays in investigation, and low conviction rates.
5. **To examine the social and institutional barriers that discourage women from reporting cybercrimes**, including fear of social stigma, victim blaming, privacy concerns, and lack of awareness about available legal remedies.
6. **To assess the role of government initiatives, specialised cybercrime units, online complaint mechanisms, and public awareness programmes** in protecting women from cybercrime and promoting digital safety.
7. **To suggest legal, administrative, and policy reforms** aimed at strengthening cybercrime prevention, improving enforcement mechanisms, enhancing victim support services, and ensuring effective protection of women's rights in the digital environment.

7. Research Methodology

7.1. Research Design

The present study adopts a **doctrinal (library-based) research methodology** to examine the legal framework governing cybercrime against women in India and to evaluate the gap between legal protection and effective enforcement. The research is analytical and descriptive in nature,

focusing on the interpretation of statutory provisions, judicial decisions, government policies, and scholarly opinions relating to cybercrime against women.

7.2. Nature of the Study

The study is **descriptive and analytical**. It describes the various forms of cybercrime committed against women, analyses the existing legal framework, and critically evaluates the effectiveness of enforcement mechanisms. The research also identifies practical challenges faced by victims, law enforcement agencies, and the judiciary in combating cybercrime.

7.3 Sources of Data

The research is based entirely on **secondary data**, collected from reliable and authoritative sources.

7.4. Primary Sources

The primary legal sources include:

- The Constitution of India.
- The Information Technology Act, 2000.
- The Bharatiya Nyaya Sanhita, 2023.
- The Bharatiya Nagarik Suraksha Sanhita, 2023.
- The Bharatiya Sakshya Adhiniyam, 2023.
- Relevant rules, notifications, and government guidelines.
- Judicial decisions of the Supreme Court of India and various High Courts relating to cybercrime, privacy, electronic evidence, and protection of women.

7.5. Secondary Sources

The secondary sources include:

- Books on cyber law, criminal law, and information technology law.

- Research articles published in peer-reviewed journals.
- Reports of the National Crime Records Bureau (NCRB).
- Publications of the Ministry of Home Affairs and the Indian Cyber Crime Coordination Centre (I4C).
- Reports of the National Commission for Women (NCW).
- Government publications, policy papers, conference proceedings, and reliable academic websites.

7.6. Method of Data Collection

Data has been collected through an extensive review of legal literature, statutes, judicial precedents, government reports, journal articles, and other published materials. The collected information has been systematically organised and analysed to understand the legal provisions, enforcement mechanisms, and practical challenges associated with cybercrime against women.

7.7. Scope of the Study

The study focuses on cybercrimes committed against women in India and examines the adequacy of existing legal protections and their practical implementation. It evaluates the role of investigative agencies, cybercrime police stations, forensic laboratories, the judiciary, and government initiatives in addressing cyber offences. The research also analyses the social factors that influence the reporting and investigation of cybercrimes against women.

7.8. Limitations of the Study

The study is limited to doctrinal research based on secondary sources and does not include empirical fieldwork such as surveys or interviews with victims, police officers, or judicial officials. As cyber technology and digital offences continue to evolve rapidly, new legal developments and technological changes occurring after the completion of this study may not be fully reflected. Nevertheless, the research provides a comprehensive analysis of the current legal framework and enforcement challenges relating to cybercrime against women in India.

8. Legal Framework Governing Cybercrime Against Women in India

The rapid growth of digital technology has transformed communication, commerce, education, and social interaction in India. However, it has also led to an alarming increase in cybercrimes, particularly those targeting women. Cyberstalking, cyberbullying, identity theft, online impersonation, revenge pornography, sextortion, morphing of images, online sexual harassment, and financial fraud have become common forms of digital violence against women. Recognising these challenges, India has developed a legal framework comprising constitutional guarantees, cyber-specific legislation, criminal laws, procedural laws, and institutional mechanisms aimed at preventing cybercrime and protecting women's rights in the digital environment.

8.1. Constitutional Protection

The Constitution of India provides the foundation for protecting women against cybercrime by guaranteeing fundamental rights that apply both offline and online.

8.1.1. Article 14 – Right to Equality

Article 14 guarantees equality before the law and equal protection of the laws. Women who become victims of cybercrime are entitled to equal protection and equal access to justice without discrimination.¹

8.1.2 Article 15(3) – Protective Discrimination

Article 15(3) empowers the State to make special provisions for women and children. This constitutional provision enables the Government to enact laws and policies specifically aimed at protecting women from cyber offences.²

8.1.3 Article 19(1)(a) – Freedom of Speech and Expression

While citizens enjoy freedom of speech and expression, this right is subject to reasonable restrictions under Article 19(2). Online speech involving harassment, obscenity, defamation,

¹ *Constitution of India, art. 14.*

² *Constitution of India, art. 15(1) & 15(3).*

hate speech, or threats against women is not protected.³

8.1.4. Article 21 – Right to Life and Personal Liberty

The Supreme Court has interpreted Article 21 to include the right to privacy, dignity, reputation, and personal security. Cybercrimes such as non-consensual sharing of intimate images, cyberstalking, and identity theft directly violate these constitutional rights.⁴

8.2. Information Technology Act, 2000

The Information Technology Act, 2000, is India's principal legislation dealing with cyber offences and electronic governance. Several provisions are particularly relevant to crimes committed against women.

8.2.1. Section 66C – Identity Theft

This provision punishes fraudulent use of another person's electronic signature, password, or digital identity. Women often become victims of fake social media accounts and identity theft.

8.2.2. Section 66D – Cheating by Personation Using Computer Resources

This section criminalises online impersonation carried out through electronic communication for fraudulent purposes, including fake matrimonial profiles and online financial scams.

8.2.3. Section 66E – Violation of Privacy

This section penalises the intentional capturing, publishing, or transmission of images of a person's private areas without consent, thereby protecting women's privacy and dignity.

8.2.4. Section 67 – Publishing or Transmitting Obscene Material

It prohibits publishing or transmitting obscene electronic material and applies to online circulation of sexually explicit or offensive content.

³ *Constitution of India, art. 19(1)(a).*

⁴ *Constitution of India, art. 21.*

8.2.5. Section 67A – Sexually Explicit Material

This provision imposes stricter punishment for publishing or transmitting sexually explicit material in electronic form.

8.2.6. Section 67B – Material Depicting Children

Although primarily intended to protect children from online sexual exploitation, this provision contributes to broader cyber safety and protects girl children from digital abuse.⁵

8.3. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita (BNS), 2023 modernises India's criminal law and contains provisions applicable to cyber-enabled crimes affecting women.

The BNS criminalises offences such as criminal intimidation, stalking, voyeurism, defamation, cheating, extortion, obscenity, sexual harassment, and publication of obscene material. Many of these offences now extend to conduct committed through electronic communication and digital platforms. These provisions strengthen legal remedies available to women facing online abuse.⁶

8.4 Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 provides the procedural framework for investigation, arrest, search, seizure, collection of electronic evidence, trial, and prosecution of cyber offences. It facilitates the use of digital evidence during criminal proceedings and encourages the adoption of technology for efficient investigation and case management.⁷

8.5. Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam (BSA), 2023 recognises electronic and digital records as admissible evidence, subject to statutory requirements. Emails, social media messages, CCTV recordings, mobile phone data, digital photographs, electronic documents, and server records

⁵ *The Information Technology Act, 2000*, §§ 66C, 66E, 67, 67A & 67B.

⁶ *The Bharatiya Nyaya Sanhita, 2023*, §§ 75, 78, 79 & 351.

⁷ *The Bharatiya Nagarik Suraksha Sanhita, 2023*, §§ 173, 176 & 193.

play an increasingly important role in prosecuting cyber offences against women.⁸

9. Judicial Interpretation

Indian courts have significantly strengthened digital rights through constitutional interpretation.

In **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)**, the Supreme Court recognised privacy as a fundamental right under Article 21. This judgment provides constitutional protection against unauthorised collection, misuse, and dissemination of personal information.⁹

In **Shreya Singhal v. Union of India (2015)**, the Supreme Court struck down Section 66A of the Information Technology Act, 2000, as unconstitutional while affirming that legitimate restrictions on unlawful online activities remain enforceable through other statutory provisions.

These landmark judgments continue to shape India's cyber jurisprudence by balancing freedom of expression with privacy, dignity, and protection from online abuse.¹⁰

10. Institutional Mechanisms

India has established several institutions to strengthen cybercrime enforcement and victim assistance.

- The Indian Cyber Crime Coordination Centre (I4C) coordinates national efforts to combat cybercrime.
- The National Cyber Crime Reporting Portal enables victims to report cyber offences, including crimes against women and children.
- Specialised cybercrime police stations investigate technology-related offences.
- Cyber forensic laboratories assist in analysing electronic evidence.
- The National Commission for Women (NCW) supports women by addressing

⁸ *The Bharatiya Sakshya Adhiniyam, 2023, §§ 61–63 (provisions relating to electronic and digital records).*

⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.*

¹⁰ *Shreya Singhal v. Union of India, (2015) 5 SCC 1.*

complaints and advocating legal and policy reforms.

These institutions complement the statutory framework by improving investigation, coordination, victim support, and public awareness.

11. Challenges in the Existing Legal Framework

Despite the existence of comprehensive laws, several challenges continue to affect their effectiveness:

- Underreporting due to fear of stigma and social pressure.
- Limited digital literacy among victims.
- Shortage of trained cybercrime investigators and forensic experts.
- Delays in investigation and prosecution.
- Jurisdictional issues involving cross-border cyber offences.
- Rapid technological developments that outpace legislative reforms.
- Low conviction rates resulting from evidentiary and procedural difficulties.

12. Suggestions

The increasing incidence of cybercrime against women in India highlights the urgent need to strengthen not only the legal framework but also its effective implementation. Although India has enacted comprehensive cyber laws and established specialised enforcement mechanisms, significant challenges remain in ensuring timely investigation, prosecution, and victim protection. Based on the findings of this study, the following suggestions are proposed:

12.1. Strengthen Cyber Law Enforcement

The Government should enhance the capacity of law enforcement agencies by establishing specialised cybercrime units in every district and providing regular training to police officers, prosecutors, and judicial officers on emerging cyber threats, digital investigation techniques, and cyber forensic procedures.

12.2. Improve Digital Forensic Infrastructure

Advanced cyber forensic laboratories should be established across all States and Union Territories to ensure the timely collection, preservation, and analysis of electronic evidence. Adequate financial resources and modern technological tools should be provided to investigative agencies to improve the quality and speed of cybercrime investigations.

12.3. Enhance Legal Awareness Among Women

Public awareness campaigns should be organised through educational institutions, workplaces, community organisations, and digital media to educate women about cyber safety, privacy protection, online fraud prevention, and the legal remedies available in cases of cybercrime. Digital literacy programmes should also promote safe internet practices and responsible use of social media.

12.4. Encourage Prompt Reporting of Cybercrimes

Victims should be encouraged to report cyber offences without fear of social stigma or victim blaming. Reporting mechanisms should be made more accessible, confidential, and user-friendly. The National Cyber Crime Reporting Portal and cybercrime helplines should be widely publicised to ensure that victims can seek immediate assistance.

12.5. Strengthen Inter-Agency Coordination

Effective coordination among cybercrime police stations, forensic laboratories, internet service providers, social media platforms, financial institutions, and regulatory authorities is essential for the prompt investigation and prosecution of cyber offences. Standard operating procedures should be developed to facilitate information sharing while protecting privacy and due process.

12.6. Promote Victim-Centred Justice

The criminal justice system should adopt a victim-centred approach by ensuring confidentiality, psychological counselling, legal aid, and rehabilitation services for women affected by cybercrime. Fast-track mechanisms may be considered for serious cyber offences involving sexual exploitation, blackmail, or circulation of intimate images.

12.7. Strengthen International Cooperation

As many cybercrimes have cross-border dimensions, India should strengthen international cooperation through mutual legal assistance treaties, information-sharing arrangements, and collaboration with international law enforcement agencies. Such cooperation is essential for tracing offenders, preserving digital evidence, and prosecuting transnational cyber offences.

12.8. Regular Review and Updating of Cyber Laws

Cyber technology evolves rapidly, creating new forms of digital offences. Therefore, cyber laws should be periodically reviewed and updated to address emerging crimes involving artificial intelligence, deepfake technology, cryptocurrency fraud, online impersonation, and other evolving cyber threats. Continuous legislative reform will ensure that the legal framework remains effective and responsive to technological developments.

12.9. Increase Accountability of Digital Platforms

Social media companies, messaging services, and online platforms should adopt stronger mechanisms for preventing online abuse. They should establish efficient grievance redressal systems, respond promptly to lawful requests from investigative agencies, remove unlawful content without unnecessary delay, and implement measures to detect and prevent repeated online harassment while respecting applicable legal safeguards.

12.10. Promote Research and Policy Development

Universities, research institutions, and government agencies should encourage interdisciplinary research on cybercrime against women to generate evidence-based policy recommendations. Regular collection and publication of reliable data on cyber offences, reporting trends, conviction rates, and victim experiences will support informed policymaking and improve the effectiveness of legal and institutional responses.

13. CONCLUSION

Cyber crime against women has emerged as a serious challenge to privacy, dignity, equality and personal security in India. Although the Constitution, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and

the Bharatiya Sakshya Adhiniyam, 2023 provide a legal framework for addressing various forms of cyber offences, a significant gap continues to exist between legal protection and effective enforcement. Difficulties in reporting, identification of offenders, collection and preservation of electronic evidence, lack of technical expertise, under-reporting and delays in investigation and prosecution weaken the practical effectiveness of existing laws. Therefore, merely expanding the legal framework is insufficient. Effective protection requires specialised cyber investigation units, better technological infrastructure, trained law enforcement personnel, accessible complaint mechanisms, speedy judicial remedies and greater awareness among women regarding their digital rights and available remedies. A victim-centred approach should also be adopted to protect the privacy and dignity of victims during investigation and trial. Ultimately, bridging the gap between law and enforcement is essential to ensure that women can participate in the digital environment without fear, discrimination or abuse. Strengthening both legal implementation and institutional capacity is therefore necessary for creating a safer and more accountable cyberspace for women in India.

REFERENCES

1. Constitution of India, 1950.
2. Information Technology Act, 2000.
3. Bharatiya Nyaya Sanhita, 2023.
4. Bharatiya Nagarik Suraksha Sanhita, 2023.
5. Bharatiya Sakshya Adhiniyam, 2023.
6. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
7. Vishaka v. State of Rajasthan, (1997) 6 SCC 241.
8. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
9. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
10. National Crime Records Bureau, Crime in India, Ministry of Home Affairs, Government of India.

BIBLIOGRAPHY

BOOKS

1. Vakul Sharma, Information Technology Law and Practice, Universal Law Publishing.
2. Pavan Duggal, Cyber Law, LexisNexis.
3. R.K. Bangia, Cyber Law, Allahabad Law Agency.
4. Aparna Chandra, Cyber Crimes and Cyber Laws, Universal Law Publishing.

STATUTES AND GOVERNMENT PUBLICATIONS

5. The Constitution of India, Government of India.
6. The Information Technology Act, 2000, Government of India.
7. The Bharatiya Nyaya Sanhita, 2023, Government of India.
8. The Bharatiya Nagarik Suraksha Sanhita, 2023, Government of India.
9. The Bharatiya Sakshya Adhiniyam, 2023, Government of India.

10. National Crime Records Bureau, Crime in India, Ministry of Home Affairs, Government of India.

ONLINE SOURCES

11. Ministry of Electronics and Information Technology, Government of India, publications relating to cyber law and cyber security.
12. National Cyber Crime Reporting Portal, Government of India.
13. National Crime Records Bureau, official crime statistics and reports.