



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

A CRITICAL STUDY ON CYBERCRIME LAWS FOR PROTECTION OF WOMEN

AUTHORED BY - JEBASINGH F

Chapterization

Chapter – I

- 1.1 Introduction
- 1.2 Significance of the Study
- 1.3 Review of Literature
- 1.4 Research Gap
- 1.5 Objectives of the Study
- 1.6 Research Question
- 1.7 Research Methodology
- 1.8 Limitations of the Study
- 1.9 Scheme of the Study

Chapter – II - CONCEPTUAL FRAMEWORK OF CYBERCRIME AGAINST WOMEN

- 2.1 Introduction
- 2.2 Meaning of Cybercrime
- 2.3 Evolution of Cybercrime
- 2.4 Nature of Cybercrime against Women
- 2.5 Challenges faced by Women Victims of Cybercrime
- 2.6 Conclusion

Chapter – III – LEGAL FRAMEWORK FOR PROTECTION OF WOMEN AGAINST CYBERCRIME IN INDIA

- 3.1 Introduction
- 3.2 Constitutional Protection of Women in Cyberspace
- 3.3 Information Technology Act, 2000
- 3.4 Section 66A and Its Judicial History

- 3.5 Bharatiya Nyaya Sanhita, 2023
- 3.6 Bharatiya Nagarik Suraksha Sanhita, 2023
- 3.7 Bharatiya Sakshya Adhiniyam, 2023
- 3.8 National Cyber Crime Reporting Mechanism
- 3.9 Overall Assessment of the Indian Legal Framework

Chapter – IV – CRITICAL ANALYSIS OF CYBERCRIME LAWS FOR PROTECTION OF WOMEN

- 4.1 Introduction
- 4.2 Effectiveness of the Information Technology Act
- 4.3 Judicial Approach Towards Cybercrime Against Women
- 4.4 Investigation of Cybercrime Against Women
- 4.5 Digital Evidence and Its Challenges
- 4.6 Jurisdictional Challenges
- 4.7 Critical Assessment of Enforcement Mechanisms

Chapter – V – FINDINGS, SUGGESTIONS AND CONCLUSION

- 5.1 Introduction
- 5.2 Suggestions and Recommendations
- 5.3 Scope of Future Research
- 5.4 Conclusion

Table of Cases

- 1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- 2. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

ABSTRACT

The rapid growth of technology has led to increasing cybercrimes against women, including cyberstalking, harassment, sextortion, identity theft, doxxing, and AI-generated deepfakes. These crimes threaten women's privacy, dignity, safety, and mental well-being. India has enacted laws such as the Information Technology Act, 2000, and the new criminal and data protection laws to address such offenses. However, underreporting, lack of awareness, anonymous offenders, digital evidence issues, and delays continue to limit effective protection. This study examines India's cybercrime laws, identifies existing gaps, and suggests reforms to strengthen women's digital safety and access to justice.

Keywords: Cybercrime, Women, Cyber Law, Information Technology Act, Bharatiya Nyaya Sanhita, Cyberstalking, Deepfake, Digital Evidence, Online Harassment, Women's Protection.

1.1 INTRODUCTION

The swift expansion of information and communication technology has revolutionized daily communication, learning, work, financial transactions, and interpersonal connectivity. While digital platforms and social media have broadened female engagement in virtual spaces, they have simultaneously given rise to novel categories of technology-driven harassment.¹

Cyber offenses frequently utilize computers, networks, digital gadgets, or the internet either as the primary target, the instrument, or the setting for criminal activity. Due to their borderless, remote, and anonymous traits, investigating authorities face major hurdles when tracking perpetrators, securing electronic evidence, determining legal jurisdiction, and securing convictions.² Women are disproportionately exposed to online infractions such as cyberstalking, cyberbullying, digital sexual misconduct, identity theft, sextortion, unauthorized exposure of private images, doxxing, digital defamation, and AI-driven deepfakes. Such violations severely jeopardize victims' personal privacy, self-respect, public reputation, mental health, and financial stability.

India has established a comprehensive legislative framework to address these digital crimes through key statutes: the Information Technology Act of 2000, the Bharatiya Nyaya Sanhita of 2023, the Bharatiya Nagarik Suraksha Sanhita of 2023, the Bharatiya Sakshya Adhiniyam of

¹ Information Technology Act, 2000, Act No. 21 of 2000; United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 2: Computer-related Offences*.

² United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 2: Introduction to Cybercrime*, discussing the borderless and technology-enabled nature of cybercrime and challenges of investigation and evidence.

2023, and the Digital Personal Data Protection Act of 2023. Enforcement is further supported by specialized law enforcement divisions, reporting portals, forensic laboratories, judicial systems, and online intermediaries.

Consequently, this research investigates the adequacy of India's legislative mechanisms in safeguarding women from digital crime, with specific emphasis on modern challenges like deepfakes and artificial intelligence abuse.

1.2 Significance of the Study

The expansion of internet connectivity, digital communication tools, social media networks, and virtual financial platforms has amplified female participation in online environments while concurrently leaving women vulnerable to tech-based offenses, including cyberstalking, cyberbullying, digital sexual misconduct, identity theft, sextortion, and the unauthorized publication of private media.

Digital violations targeting women transcend traditional criminal jurisprudence, engaging broader constitutional issues concerning personal privacy, human dignity, equality, social reputation, individual liberty, and equitable legal recourse. Because the right to privacy is constitutionally guaranteed as a fundamental freedom under Article 21 of the Constitution of India, safeguarding citizens against the exploitation of personal data and digital footprints assumes heightened legal significance.³

India addresses these issues through an established legislative and operational matrix comprising the Information Technology Act of 2000, the Bharatiya Nyaya Sanhita of 2023, the Bharatiya Nagarik Suraksha Sanhita of 2023, the Bharatiya Sakshya Adhiniyam of 2023, and the Digital Personal Data Protection Act of 2023, alongside institutional grievance channels such as the National Cyber Crime Reporting Portal.⁴

Consequently, this study holds critical importance as it assesses both the theoretical framework and the operational efficacy of current cyber regulations, pinpointing systemic bottlenecks and proposing viable reforms to fortify online safety protocols for women.

1.3 Review of Literature

1. Aparna Viswanathan – *Cyber Law: Indian and International Perspectives*

Viswanathan discusses the development of cyber law, digital offenses, electronic transactions,

³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; Constitution of India, art. 21.

⁴ Information Technology Act, 2000 (Act No. 21 of 2000); Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023); Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023); Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023); Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

and intermediary responsibilities. However, the book gives limited attention to gender-specific cybercrimes and the practical enforcement challenges faced by women.

2. Pavan Duggal – *Cyber Law: The Indian Perspective*

Duggal examines the Information Technology Act, 2000, cyber offenses, electronic records, digital signatures, privacy, and investigation. Its coverage of technology-based crimes against women and emerging threats such as deepfakes is limited.

3. Justice Yatindra Singh – *Cyber Laws*

Singh explains cyber regulations, e-governance, online offenses, and relevant judicial decisions. However, it mainly addresses general cybercrime rather than the specific protection of women from online abuse.

4. Jagadhish Raju B. & V. Karthikeyan (2026)

Their study examines constitutional safeguards, cyber laws, intermediary rules, and institutional measures for protecting women online. It identifies gaps in implementation, public awareness, digital forensics, victim support, and timely justice.

5. Priyanka Sethi (2025)

Sethi analyzes the Bharatiya Nyaya Sanhita, 2023, with particular focus on women's rights and sexual offenses. The study highlights continuing challenges in technological investigation, victim support, and institutional implementation.

6. Government and NCRB Publications

Government and NCRB reports provide information on cybercrime trends affecting women and emphasize the need for stronger enforcement, improved forensic facilities, public awareness, and better coordination among authorities and online platforms.

1.4 Research Gap

Although India possesses established digital legislation—such as the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita of 2023—existing academic literature largely restricts itself to outlining statutory sections without critically assessing how effectively these laws safeguard women.⁵ Current scholarship exhibits a notable absence of deep investigation into modern dangers, including artificial intelligence-driven deepfakes, AI impersonation, and cross-border cyber offenses. Furthermore, sufficient academic attention has not been paid to operational hurdles such as investigative backlogs, the complexities surrounding electronic evidence handling, and dismal conviction rates. Additionally, there is a scarcity of comparative

⁵ Information Technology Act, 2000 (Act No. 21 of 2000); Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).

evaluations against foreign legislative models, alongside a lack of focus on survivor rehabilitation frameworks and digital literacy programs tailored for women. To bridge these deficits, this study undertakes a critical appraisal of India's cybercrime statutes, law enforcement protocols, and judicial outcomes, ultimately putting forward actionable legal reforms to secure stronger, more comprehensive protections for women in virtual.⁶

1.5 Objectives of the Study

1. **Evaluate the effectiveness of India's cyber laws** in protecting women from digital crimes.
2. **Examine legal safeguards** under major Indian cyber and criminal laws.
3. **Assess reporting, investigation, and prosecution mechanisms** for cybercrimes against women.
4. **Identify challenges faced by women victims**, including stigma, anonymity, digital evidence, and delays.
5. **Recommend legal and institutional reforms** to address emerging threats like AI deepfakes and improve victim protection.

1.6 Research Questions

The following research questions will guide the study:

1. What are the principal manifestations and defining features of technology-facilitated crimes targeting women in India?
2. What constitutional guarantees and statutory protections currently exist to safeguard women from digital abuse?
3. Do the established provisions within the Information Technology Act, 2000 offer sufficient legal recourse against cybercrimes aimed at women?
4. How efficiently do the newly introduced provisions of the Bharatiya Nyaya Sanhita, 2023 tackle cyber-enabled offenses against women?
5. How do the procedural and evidentiary frameworks under the Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023 impact the investigation and prosecution of digital crimes?
6. What are the primary systemic and social barriers female victims encounter when filing complaints and seeking legal redress for cyber offenses?

⁶ National Crime Records Bureau, *Crime in India* reports; Information Technology Act, 2000; Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).

7. How functional and reliable are current law enforcement operations and specialized investigative mechanisms in handling cybercrime?

1.7 Research Methodology

This study adopts a **doctrinal, analytical, and comparative legal methodology** to examine the effectiveness of India's legal framework for protecting women from cybercrime. The doctrinal approach focuses on the study of primary legal sources, including the Constitution of India, Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, Digital Personal Data Protection Act, 2023, relevant rules, official reports, and judicial decisions. Secondary sources include books, journal articles, research papers, and policy publications.⁷

The analytical approach evaluates the **scope, effectiveness, and limitations** of existing laws in addressing cyberstalking, harassment, identity theft, sextortion, image-based abuse, doxxing, digital defamation, and AI-generated deepfakes. It also examines judicial approaches to privacy, dignity, electronic evidence, victim protection, reporting, evidence preservation, offender anonymity, jurisdiction, and enforcement delays.

The study is primarily **qualitative**, using legal interpretation and judicial analysis rather than original empirical data. Government statistics and institutional reports are used to provide background on cybercrime trends. The research ultimately identifies legal and procedural gaps and proposes **legislative, technological, and victim-centred reforms** to strengthen women's digital safety in India.

1.8 Limitations of the Study

Certain constraints apply to the scope and execution of this study. Given its primarily doctrinal nature, the research does not incorporate empirical field studies or direct interviews with victims. Furthermore, because digital technology evolves rapidly, novel categories of cyber-offenses may surface beyond the parameters of this analysis. The work relies predominantly on published literature and official government statistics, which may not fully reflect the true scale of incidents due to dark figure of crime factors—such as social stigma, victim intimidation, lack of awareness, fear, and privacy concerns that drive underreporting.⁸

⁷ Constitution of India; Information Technology Act, 2000 (Act No. 21 of 2000); Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023); Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023); Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023); Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

⁸ National Crime Records Bureau, *Crime in India* reports; National Cyber Crime Reporting Portal, Government of India.

While selected international models are reviewed for comparative perspective, the primary analytical focus remains centered on the Indian legal regime. Access constraints regarding confidential police records, internal forensic reports, and detailed prosecution files present additional boundaries. Moreover, because jurisprudence surrounding artificial intelligence, deepfakes, and synthetic media is actively evolving, ongoing legislative and judicial updates may emerge beyond the timeframe of this evaluation. Lastly, this inquiry is strictly restricted to cybercrimes targeted at women and does not attempt to address all general classifications of computer-related crime in India.

1.9 Scheme of the Study

The research, titled “*A Critical Study on Cybercrime Laws for Protection of Women*,” is organized into five chapters. It progresses from the conceptual understanding of cybercrime to legal analysis, critical evaluation, and recommendations.

Chapter I – Introduction:

This chapter introduces the background, scope, and significance of cybercrime against women. It presents the problem statement, rationale, literature review, objectives, research questions, methodology, and limitations of the study.

Chapter II – Conceptual Framework of Cybercrime Against Women:

This chapter explains the meaning, development, and major forms of cybercrime affecting women, including cyberstalking, harassment, cyberbullying, identity theft, sextortion, doxxing, digital extortion, image-based abuse, and AI-generated deepfakes. It also examines their psychological, social, and economic effects and the difficulties faced by victims in reporting such crimes.

Chapter III – Legal Framework for Protection of Women Against Cybercrime in India:

This chapter examines constitutional safeguards and major laws governing cybercrime, including the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, and Digital Personal Data Protection Act, 2023. It also considers the role of cybercrime reporting portals, law-enforcement agencies, forensic units, courts, and digital intermediaries.⁹

Chapter IV – Critical Analysis of Cybercrime Laws for Protection of Women:

This chapter evaluates the effectiveness and limitations of the existing legal framework. It

⁹ Information Technology Act, 2000 (Act No. 21 of 2000); Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023); Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023); Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023); Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

considers judicial decisions, digital evidence, forensic procedures, anonymity of offenders, jurisdictional challenges, enforcement delays, underreporting, victim privacy, compensation, and emerging threats such as AI-generated deepfakes. Comparative legal practices are also considered.¹⁰

Chapter V – Suggestions and Conclusion:

The final chapter summarizes the major findings and identifies strengths and gaps in the existing framework. It provides recommendations for improving legislation, cyber-forensic facilities, victim support, digital literacy, regulation of synthetic media, and international cooperation. It concludes by emphasizing the need for a responsive and victim-centred legal system to address evolving cyber threats against women.

CHAPTER II

CONCEPTUAL FRAMEWORK OF CYBERCRIME AGAINST WOMEN

The rapid advancement of information and communication technology has transformed various aspects of modern life, including communication, employment, education, financial activities, and social interaction. The widespread use of the internet and social media has made digital platforms an integral part of everyday life. Women are increasingly relying on these platforms for educational opportunities, employment, entrepreneurship, entertainment, communication, and participation in society. At the same time, greater involvement in the digital environment has increased women's exposure to different forms of technology-facilitated crime and abuse. Cybercrime targeting women has emerged as a significant social and legal concern. Digital technologies can be exploited to harass, intimidate, threaten, exploit, defame, stalk, or sexually abuse women. Unlike many conventional offences, cybercrimes can be carried out remotely, often making it difficult to identify the offender. Furthermore, harmful digital material can be reproduced, altered, and distributed rapidly, allowing its impact to spread to a large audience within a short period.¹¹

The continuous evolution of technology has further complicated the nature of cybercrime. Developments such as artificial intelligence, deepfake technology, synthetic media, encrypted communication, and other advanced digital tools have introduced new ways in which offences against women can be committed. Consequently, a clear understanding of the concept, nature, and various forms of cybercrime is necessary before analysing the legal mechanisms

¹⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

¹¹ United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 2: Introduction to Cybercrime*.

established to protect women from such offences.

This chapter focuses on the meaning, nature, characteristics, and development of cybercrime against women. It further examines the major forms of cybercrime that affect women and analyses their psychological, social, and economic consequences.

2.2 Meaning of Cybercrime

Cybercrime can broadly be described as illegal or harmful activities carried out through computers, smartphones, digital devices, electronic networks, or the internet. In such offences, a digital device or computer system may itself be the object of attack, serve as a tool for carrying out the offence, or provide the digital setting in which the unlawful activity takes place.¹²

One of the distinguishing features of cybercrime is that the individuals involved do not necessarily need to be present in the same physical location. An offender may conceal their identity by using false credentials, anonymous profiles, or other digital means. In many cases, the person responsible may be operating from a different State or from outside the country, creating additional challenges for investigation and enforcement.

In this context, cybercrime against women may be understood as unlawful, threatening, or abusive behaviour conducted through digital technologies and directed towards women, or having a particularly significant impact on them on account of their gender. Such offences can take several forms, including online harassment, threats and intimidation, sexual exploitation, invasion of privacy, financial misconduct, damage to reputation, and psychological or emotional abuse.¹³

2.3 Evolution of Cybercrime

The emergence and progression of cybercrime have closely followed the development of computers and the internet. During the early period of computerisation, digital offences were largely limited to activities such as gaining unauthorised access to computer systems, spreading malicious software, stealing information, and altering or damaging digital data.

As internet usage expanded, cybercriminal activities became increasingly complex and diverse. Offences involving fraudulent emails, hacking, identity-related crimes, and illegal financial transactions became more widespread. The emergence of social media further transformed the digital environment by enabling people to communicate, interact, and distribute information

¹² Information Technology Act, 2000 (Act No. 21 of 2000); United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 2: Computer-related Offences*.

¹³ United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 2: Introduction to Cybercrime*.

almost instantaneously. Recent technological advancements have created additional challenges in addressing cybercrime. Artificial intelligence can now be used to produce highly realistic images, videos, and audio recordings. Consequently, deepfake technology may be exploited to fabricate sexual, misleading, or defamatory content involving women. The continuing emergence of such technologies illustrates that cybercrime is an evolving phenomenon that changes alongside advancement in the digital world.

2.4 Nature of Cybercrime Against Women

Cybercrime directed against women possesses several distinctive features that make it different from many forms of conventional criminal activity. The digital nature of such offences creates particular challenges relating to the identity of offenders, geographical boundaries, dissemination of harmful material, preservation of evidence, and the consequences suffered by victims.

2.4.1 Anonymity

Cyber offenders can conceal their identities by using fabricated profiles, pseudonyms, disposable email accounts, virtual telephone numbers, and other digital techniques. Such methods can make it difficult for law-enforcement authorities to establish the actual identity of the offender and trace the source of the offence.¹⁴

2.4.2 Remote Commission of Crime

Physical proximity between the offender and the victim is not required for a cyber offence to take place. An offender situated in a different city, State, or country can target a woman through social media, messaging applications, email, or other online platforms.

2.4.3 Rapid Dissemination

Information shared through digital platforms can reach a very large audience within a matter of minutes. Harmful, intimate, or defamatory material can be repeatedly copied, forwarded, and uploaded on different platforms, making it extremely difficult to control its circulation once it becomes publicly available.¹⁵

2.4.4 Persistence of Digital Content

Removing offensive content from its original source does not necessarily eliminate it from the internet. Duplicate copies may continue to exist on websites, electronic devices, cloud storage,

¹⁴ United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 2: General Types of Cybercrime*, discussing the borderless nature of cybercrime, anonymity of offenders, and the challenges involved in identifying and tracing perpetrators.

¹⁵ UNODC, *Cybercrime Module 2: General Types of Cybercrime*, explaining the rapid and wide dissemination of information through digital technologies and the difficulties in controlling electronically distributed content.

or other online accounts. As a result, the consequences of the offence may continue long after the original material has been removed.

2.4.5 Cross-Border Character

Cyber offences can extend across national boundaries, with the offender, victim, digital platform, and computer servers potentially situated in different countries. Such circumstances can create significant difficulties concerning jurisdiction, investigation, collection of evidence, and cooperation between law-enforcement agencies.

2.4.6 Psychological Impact

Technology-facilitated abuse can have serious effects on the mental and emotional well-being of women. Victims may experience fear, embarrassment, anxiety, social withdrawal, emotional distress, and diminished self-confidence. Repeated messages, threats, or online monitoring can also create a continuing sense of insecurity.¹⁶

2.5 Challenges Faced by Women Victims of Cybercrime

Women who become victims of cybercrime encounter a range of legal, social, technological, and psychological obstacles while attempting to obtain justice and appropriate remedies. Although several laws, institutions, and mechanisms exist to address cyber offences, victims may face difficulties at different stages, including reporting the incident, investigation, prosecution, and obtaining relief. The borderless nature of cyberspace, concealed identities of offenders, rapid distribution of digital material, and involvement of multiple jurisdictions can further complicate the process. These factors may discourage victims from approaching authorities and contribute to the under-reporting of cyber offences. The principal challenges experienced by women victims are discussed below.

1. Lack of Awareness

Insufficient knowledge about legal rights and available remedies is one of the major obstacles faced by women affected by cybercrime. Victims may not always recognise that certain online behaviour constitutes a punishable offence or may be uncertain about the legal provisions that apply to their circumstances. A woman subjected to cyberstalking, online harassment, identity theft, impersonation, threatening communications, or unauthorised sharing of intimate images may not know the appropriate authority or legal procedure for making a complaint. Limited knowledge about cybercrime reporting portals, specialised police units, and other complaint mechanisms can further discourage or delay reporting. Victims may also be unaware that digital

¹⁶ UN Women, *Online and ICT-Facilitated Violence Against Women and Girls During COVID-19*, discussing the psychological and social consequences of technology-facilitated violence against women

material such as screenshots, messages, URLs, account information, and other electronic records should be preserved as potential evidence. Increasing legal awareness and digital literacy can therefore help women identify cyber offences, protect relevant evidence, and seek appropriate assistance at an early stage.¹⁷

2. Fear and Social Stigma

Social stigma and fear of judgement can significantly influence a woman's decision to report a cybercrime. Victims of online sexual harassment, cyberstalking, sextortion, intimate-image abuse, and other privacy-related offences may worry about how their family, friends, colleagues, or wider society will respond. Feelings of shame, embarrassment, and concern about reputational damage may prevent victims from seeking assistance. Offenders may intentionally exploit these concerns by threatening to release private photographs, videos, conversations, or personal information unless the victim follows their demands. Consequently, some women may choose not to disclose the offence or may discontinue a complaint despite experiencing considerable emotional and social consequences. Social stigma can therefore benefit offenders by reducing the likelihood of their activities being reported. Confidential, accessible, and victim-sensitive complaint procedures are important for creating an environment in which women can report cyber offences without fear of humiliation or victim-blaming.

3. Anonymous Offenders and Difficulty in Identification

The ability to conceal one's identity online presents a significant challenge to the investigation of cybercrime. Offenders can create fraudulent social media profiles, use assumed identities, temporary email accounts, virtual private networks, altered images, and other technological methods to hide their identity. They may also operate from a different geographical location and use several accounts or electronic devices while committing the offence. Tracing such individuals may require specialised digital investigation and examination of information such as IP addresses, device records, account details, electronic communications, and other available digital traces. In some cases, offenders may deactivate accounts, delete information, or employ additional methods to make identification more difficult.¹⁸ These circumstances can make cybercrime investigations technically demanding and may prolong the process of identifying and prosecuting the person responsible.

¹⁷ Government of India, Ministry of Home Affairs, *National Cyber Crime Reporting Portal*, providing information on reporting cybercrime complaints and mechanisms available to victims.

¹⁸ Information Technology Act, 2000, §§ 43, 66, 66C, 66D and 66E, concerning unauthorised access, computer-related offences, identity theft and related forms of misuse of digital technology.

4. Problems Relating to Digital Evidence

Electronic evidence is often central to the investigation and prosecution of cyber offences, yet preserving such evidence can be challenging. Messages, emails, photographs, videos, social media content, call records, and website information may be altered, deleted, or otherwise lost within a short period. Victims may also unintentionally destroy relevant evidence by deleting conversations, replacing devices, or failing to preserve the original material. For digital evidence to be relied upon during legal proceedings, its authenticity and integrity may need to be established. Investigating authorities must therefore collect, preserve, and examine electronic evidence using appropriate procedures. Additional difficulties can arise when relevant information is held by technology companies or stored on servers located outside India. Proper and timely preservation of digital evidence is consequently essential for effective investigation and successful prosecution of cybercrime cases.¹⁹

5. Jurisdictional Problems

The borderless nature of the internet can create complex questions concerning jurisdiction. A cyber offence may involve a victim in one location, an offender in another State or country, and digital platforms or servers situated elsewhere. For example, an offence against a woman in India may be committed by an individual located outside the country, while important electronic evidence may be stored on foreign servers. Such circumstances can make it difficult to determine the appropriate investigating authority and obtain necessary information from foreign authorities or private technology companies. International cases may require cooperation between different law-enforcement agencies and compliance with separate legal procedures. These jurisdictional complications can delay investigations and make it more difficult for victims to obtain timely and effective remedies.²⁰

6. Difficulty in Removing Harmful Content

The permanent or recurring availability of harmful online material presents another major challenge for women victims. Intimate photographs, videos, manipulated images, defamatory content, or private information may be removed from the platform on which they were initially posted after a complaint. However, the material may already have been downloaded, copied, forwarded, or uploaded elsewhere. Consequently, removing the original content does not necessarily prevent its continued circulation. Repeated exposure to such material can cause

¹⁹ Bharatiya Sakshya Adhiniyam, 2023, provisions relating to the admissibility and proof of electronic or digital records; Information Technology Act, 2000.

²⁰ Information Technology Act, 2000; United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 7: Cybercrime Investigation*, discussing jurisdictional and cross-border challenges in cybercrime investigations.

ongoing emotional distress, humiliation, and reputational harm. Victims may also need to submit multiple requests to different websites or platforms when the material is repeatedly reposted. Effective systems for prompt reporting, removal, blocking, and prevention of further distribution are therefore important for reducing the continuing harm caused by such offences.²¹

7. Lack of Adequate Legal, Psychological and Technological Support

Women affected by cybercrime may require several forms of assistance in addition to the formal filing of a criminal complaint. Offences involving sexual harassment, stalking, threats, blackmail, or intimate-image abuse can have serious emotional consequences, including fear, anxiety, psychological distress, and reduced self-confidence. Victims may consequently require counselling and emotional support alongside legal guidance.

Technological assistance can also be necessary to secure online accounts, change passwords, preserve relevant evidence, report abusive material, and prevent further misuse of personal information. However, such comprehensive support may not always be readily accessible, particularly to women with limited financial resources or digital knowledge. A victim-centred system should therefore seek to provide coordinated legal, psychological, and technological assistance, enabling women to navigate the reporting and justice process safely and effectively.²²

2.6 Conclusion

Cybercrime against women is a multifaceted issue that continues to develop alongside advancements in digital technology. The widespread adoption of social media, smartphones, online communication systems, and artificial intelligence has expanded opportunities for positive social and economic activities while simultaneously creating new avenues for digital abuse and criminal conduct. Women may be subjected to various forms of cybercrime, including cyberstalking, cyberbullying, online sexual harassment, cyber defamation, identity theft, impersonation, sextortion, unauthorised distribution of intimate images, image morphing, doxxing, blackmail, and the creation or circulation of AI-generated deepfakes.

The effects of these offences extend beyond the online sphere and can have significant consequences for the victim's mental well-being, dignity, privacy, personal relationships,

²¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, concerning grievance redressal and obligations relating to removal of specified unlawful content.

²² United Nations Women, *Online and ICT-Facilitated Violence Against Women and Girls*, discussing the need for survivor-centred responses and appropriate support mechanisms for women experiencing technology-facilitated violence.

education, employment, and financial security. A clear understanding of the nature and different forms of cybercrime against women is therefore essential for assessing the legal measures available to prevent such offences, protect victims, and provide effective remedies. The conceptual foundation established in this chapter serves as a basis for examining the relevant legal framework in the subsequent discussion.

CHAPTER III

LEGAL FRAMEWORK FOR PROTECTION OF WOMEN AGAINST CYBERCRIME IN INDIA

3.1 INTRODUCTION

The rapid advancement of digital technologies has made the establishment of a strong and effective legal framework essential for protecting individuals from cyber offences. Women may require particular attention within this framework as they can be exposed to various technology-facilitated offences, including cyberstalking, online sexual harassment, impersonation, sextortion, unauthorised dissemination of intimate images, cyber defamation, identity theft, image morphing, doxxing, and the creation or distribution of AI-generated deepfake material.

In India, laws relating to cybercrime are not consolidated within one comprehensive legislation. Instead, the legal framework consists of several interconnected sources, including constitutional protections, criminal statutes, information technology laws, procedural legislation, laws governing electronic evidence, data protection legislation, intermediary-related regulations, and institutional mechanisms established to address cyber offences.

The Information Technology Act, 2000 continues to constitute a significant part of India's legal framework for addressing offences involving information technology and electronic communication. The Bharatiya Nyaya Sanhita, 2023 establishes the substantive criminal law framework, whereas the Bharatiya Nagarik Suraksha Sanhita, 2023 governs criminal investigation and procedural matters. The Bharatiya Sakshya Adhiniyam, 2023 provides the evidentiary framework, including provisions concerning electronic and digital records. In addition, the Digital Personal Data Protection Act, 2023 is relevant to the regulation and protection of personal data in the digital environment.²³

The mere existence of legislation, however, does not by itself guarantee effective protection

²³ Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; Digital Personal Data Protection Act, 2023.

for victims. The practical effectiveness of the legal framework depends upon its proper enforcement, efficient investigation, availability of digital forensic expertise, appropriate judicial intervention, coordination among relevant institutions, and adequate support and assistance for victims. A coordinated approach involving these elements is essential for ensuring meaningful protection and effective remedies for women affected by cybercrime.

3.2 Constitutional Protection of Women in Cyberspace

The Constitution of India forms the basic legal foundation for safeguarding women from various forms of cybercrime. Although the Constitution predates the emergence of the internet and contemporary digital technologies, its principles concerning equality, individual liberty, human dignity, and privacy remain applicable to conduct occurring in the digital sphere.²⁴

3.2.1 Article 14 – Equality Before Law

Article 14 establishes the constitutional principle of equality before the law and equal protection of the laws. Women subjected to cyber offences are consequently entitled to equal treatment and access to appropriate legal remedies. Police authorities, investigative agencies, and courts are required to address complaints of cybercrime without discrimination and with due seriousness. The guarantee of equality also provides a constitutional basis for developing measures that respond effectively to gender-based violence and abuse in digital spaces.

3.2.2 Article 15 – Prohibition of Discrimination

Article 15 prohibits discrimination on specified grounds, including sex. Certain forms of cyber abuse may specifically target women because of their gender. Conduct such as online sexual harassment, gender-based intimidation, and sexually abusive digital communications can restrict women's ability to participate freely and equally in online and public spaces. The constitutional protection under Article 15 therefore supports measures aimed at ensuring women's safety, equality, and meaningful participation in cyberspace.²⁵

3.2.3 Article 19 – Freedom of Speech and Expression

Article 19(1)(a) guarantees citizens the fundamental right to freedom of speech and expression. Digital platforms, particularly social media and online communication services, have become significant means through which women exercise this right. They enable women to express views, engage in public discourse, operate businesses, exchange information, and communicate with others.

²⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, recognising privacy as a constitutionally protected right under Article 21 and affirming the broader constitutional protection of dignity and liberty.

²⁵ Constitution of India, art. 15, prohibiting discrimination on specified grounds, including sex.

The freedom guaranteed under Article 19 is not absolute. Article 19(2) permits reasonable restrictions on the exercise of this right in specified circumstances. Consequently, conduct such as unlawful threats, cyberstalking, defamatory communications, and other criminal forms of online abuse cannot automatically claim constitutional protection as freedom of expression. The legal framework must therefore preserve legitimate online expression while providing protection against unlawful digital conduct.²⁶

3.2.4 Article 21 – Right to Life and Personal Liberty

Article 21 protects the right to life and personal liberty by providing that no person shall be deprived of these rights except in accordance with a procedure established by law. Through judicial interpretation, the scope of Article 21 has expanded to encompass several dimensions of human dignity, privacy, and individual autonomy.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court affirmed that the right to privacy forms part of the fundamental rights protected by the Constitution. This constitutional recognition has particular significance in the context of cybercrime against women. Unauthorised dissemination of intimate photographs, misuse of personal information, digital surveillance, and similar forms of online intrusion can adversely affect an individual's privacy, dignity, and personal autonomy. Protection from cybercrime is therefore closely associated with the constitutional guarantees contained in Article 21.

3.3 Information Technology Act, 2000

The Information Technology Act, 2000 constitutes a major component of India's legal framework concerning cyberspace and electronic activities. The legislation provides legal recognition to electronic records and electronic transactions and contains provisions dealing with various forms of unlawful conduct involving computer systems and electronic communication. Several provisions are particularly relevant when considering the protection of women from cyber offences.

3.4 Section 66A and Its Judicial History

Section 66A of the Information Technology Act previously created criminal liability for certain types of communications transmitted through communication services. However, the Supreme Court declared the provision unconstitutional in *Shreya Singhal v. Union of India*. The Court held that Section 66A infringed the fundamental right to freedom of speech and expression

²⁶ Constitution of India, arts. 19(1)(a) and 19(2); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

guaranteed under Article 19(1)(a) and could not be justified under the permissible restrictions contained in Article 19(2).

The decision has considerable significance for the development of cyber law in India. It demonstrates that legislation regulating online conduct must remain consistent with constitutional guarantees. At the same time, it highlights the challenge of distinguishing constitutionally protected online expression from communications and activities that constitute genuine cyber abuse or criminal conduct.²⁷

3.5 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) replaced the Indian Penal Code and now constitutes the principal legislation governing substantive criminal offences in India. Although the BNS is not specifically designed as legislation dealing exclusively with cybercrime, a number of offences recognised under it can be committed or facilitated through digital technologies. Cyber offences against women may involve conduct relating to sexual offences, stalking, criminal intimidation, cheating, defamation, obscenity, and other forms of criminal behaviour. Accordingly, depending upon the circumstances and nature of an offence, the provisions of the BNS may operate alongside the Information Technology Act, 2000.

3.5.1 Stalking

Stalking is recognised as a criminal offence under the BNS. With the widespread use of digital communication, stalking may occur through both physical and electronic means. Persistent monitoring, following of online activities, or repeated unwanted communication with a woman through digital platforms may raise issues relating to technology-facilitated stalking. The application of criminal law in such circumstances is significant because offenders may create multiple accounts or shift between different digital platforms to continue their conduct and evade identification.²⁸

3.5.2 Sexual Harassment

The BNS contains provisions dealing with sexual harassment. Where such conduct is carried out or facilitated through electronic communications or digital platforms, the applicability of the relevant criminal provisions will depend upon the specific facts and circumstances. In appropriate cases, the provisions of the BNS may operate together with applicable provisions of information technology legislation.

²⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

²⁸ Bharatiya Nyaya Sanhita, 2023, § 78, concerning the offence of stalking, including monitoring the use by a woman of the internet, email or other forms of electronic communication.

3.5.3 Criminal Intimidation

Digital technology can be misused to threaten women with physical injury, exposure of private photographs, disclosure of personal information, reputational harm, or other adverse consequences. Where such threats satisfy the legal requirements of criminal intimidation, the relevant provisions of the BNS may become applicable. The digital nature of the communication does not, by itself, prevent criminal law from applying to the conduct.²⁹

3.5.4 Defamation

Online platforms provide opportunities for the rapid publication and circulation of statements that may adversely affect a person's reputation. False or defamatory statements concerning a woman may therefore give rise to issues under the criminal law relating to defamation, where the necessary legal elements are established. The wide reach and rapid circulation of digital content can potentially increase the impact of reputational harm.

3.6 Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) establishes the procedural framework governing criminal investigations, inquiries, and trials. In the context of cybercrime, its relevance extends to matters such as registration and investigation of offences, search and seizure, collection and preservation of evidence, examination of witnesses, police investigation, and proceedings before criminal courts. Cybercrime cases frequently involve evidence stored on electronic devices, online accounts, computer systems, servers, and digital platforms. Effective procedural mechanisms are therefore essential to ensure that complaints involving women are dealt with appropriately and that relevant evidence is collected and preserved in accordance with law.

3.7 Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) assumes particular importance in cybercrime proceedings because electronic and digital records often constitute significant forms of evidence. Depending upon the nature of the offence, such evidence may include emails, text messages, social media communications, photographs, videos, audio recordings, call records, computer files, server information, metadata, electronic payment records, and other forms of digitally stored information. For such material to be effectively relied upon during legal proceedings, questions concerning its authenticity, reliability, integrity, and proper

²⁹ Bharatiya Nyaya Sanhita, 2023, §§ 351–352, concerning criminal intimidation and intentional insult with intent to provoke breach of peace.

preservation become important. The evidentiary framework therefore plays a crucial role in enabling courts to assess electronic records presented in cybercrime cases.³⁰

3.8 National Cyber Crime Reporting Mechanism

The Government of India has introduced the National Cyber Crime Reporting Portal to facilitate the online reporting of cyber offences. The availability of an online reporting mechanism provides victims with an additional avenue for approaching the authorities without necessarily having to begin the process by physically visiting a police station. This may be particularly beneficial to women who experience difficulties or hesitation in approaching law-enforcement authorities directly.

However, the practical effectiveness of an online cybercrime reporting system depends upon several factors, including:

- public awareness of the reporting facility;
- ease of access and user-friendliness;
- timely response to complaints;
- effective investigation;
- coordination among relevant authorities and agencies; and
- appropriate support for victims.

An accessible reporting mechanism is therefore only one component of an effective cybercrime response and must be supported by efficient investigation and victim-oriented institutional practices.³¹

3.9 Overall Assessment of the Indian Legal Framework

India has established a broad legal and institutional framework for addressing cybercrime against women. Constitutional principles relating to equality, liberty, dignity, and privacy provide the fundamental basis for protecting individuals in the digital environment. The Information Technology Act, 2000 addresses several technology-related offences, while the Bharatiya Nyaya Sanhita, 2023 contains substantive criminal provisions that may apply where criminal conduct is carried out or facilitated through digital means.

The Bharatiya Nagarik Suraksha Sanhita, 2023 establishes the procedural framework for investigation and criminal proceedings, whereas the Bharatiya Sakshya Adhiniyam, 2023 is

³⁰ Bharatiya Sakshya Adhiniyam, 2023, provisions concerning electronic or digital records and their admissibility and proof in legal proceedings.

³¹ Government of India, Ministry of Home Affairs, *National Cyber Crime Reporting Portal*, providing an online mechanism for reporting cybercrime complaints and seeking assistance from law-enforcement authorities.

significant in relation to the admissibility and assessment of electronic and digital evidence. The Digital Personal Data Protection Act, 2023 further contributes to the regulatory framework concerning the protection and processing of personal data. In addition, mechanisms such as cybercrime reporting portals, specialised cybercrime units, cyber-forensic facilities, police authorities, and the judiciary contribute to the institutional response.³²

The analysis of this legal framework provides the basis for examining its practical effectiveness. The subsequent chapter therefore focuses on the functioning of cybercrime laws, judicial responses, investigation and digital evidence, cyber-forensic practices, jurisdictional challenges, victim protection mechanisms, emerging technologies, and selected international approaches.

CHAPTER IV

CRITICAL ANALYSIS OF CYBERCRIME LAWS FOR PROTECTION OF WOMEN.

4.1 Introduction

The previous chapter discussed the constitutional, statutory and institutional measures available in India for safeguarding women from cybercrime. India has introduced various laws and institutional mechanisms to deal with offences committed through digital technologies. The Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Digital Personal Data Protection Act, 2023 collectively address different dimensions of cybercrime. However, the mere existence of legislation cannot ensure complete protection for women unless these provisions are effectively implemented. The practical success of the legal system depends on its capacity to respond to emerging forms of cybercrime, provide accessible remedies, support effective investigation and prosecution, and ensure timely justice.³³

Cybercrime against women presents distinctive challenges due to the anonymous nature of online offenders, differences in the geographical locations of victims and perpetrators, and the speed with which harmful digital material can be reproduced and distributed. The increasing use of artificial intelligence, deepfakes and synthetic media has added further complexity to the existing legal response. This chapter therefore critically analyses the strengths and shortcomings of the Indian legal framework and examines whether it is capable of addressing

³² Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023); Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023); Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

³³ Information Technology Act, 2000 (Act No. 21 of 2000); Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023); Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; Digital Personal Data Protection Act, 2023.

both established and emerging forms of cybercrime against women.

4.2 Effectiveness of the Information Technology Act

The Information Technology Act continues to constitute a significant component of India's legal response to cybercrime. Its provisions relating to identity theft, personation, privacy violations and sexually explicit electronic material are particularly relevant to offences committed against women. These provisions acknowledge the potential of digital technologies to facilitate invasion of privacy, misuse of personal information and other forms of serious harm.

The practical effectiveness of these provisions, however, is closely connected with the quality of investigation and enforcement. A statutory offence has limited practical significance where the offender cannot be identified or adequate electronic evidence cannot be obtained. For instance, an offender may establish a fraudulent online account, provide false identifying information, remove the account after committing the offence or employ technological means to conceal their identity. Consequently, the recognition of an offence under the legislation does not automatically result in successful prosecution.³⁴

Another limitation arises from the fact that the Information Technology Act was enacted in 2000, at a time when the digital environment was considerably less developed than it is today. Although subsequent amendments, rules and other legislation have strengthened the legal framework, the rapid growth of social media, artificial intelligence and other digital technologies requires continuous assessment of the Act's adequacy.

4.3 Judicial Approach Towards Cybercrime Against Women

The judiciary performs a significant function in adapting established legal principles to changing technological circumstances. Courts are required to balance the interests of victims with the rights of accused persons, intermediaries and other relevant stakeholders. Judicial decisions relating to privacy and digital rights have contributed substantially to the development of constitutional principles in this field. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognised privacy as a fundamental right. This principle assumes particular importance in cases involving the unauthorised disclosure of intimate photographs, personal information or other private material relating to women.

Judicial interpretation becomes especially significant when legislation does not expressly

³⁴ Information Technology Act, 2000, §§ 66C, 66D, 66E, 67 and 67A, concerning identity theft, cheating by personation, privacy violations, obscene material and sexually explicit material

contemplate a newly emerging form of technological abuse. Courts may interpret existing provisions consistently with constitutional principles, while also ensuring that judicial interpretation does not effectively create a new criminal offence. The judgment in *Shreya Singhal v. Union of India* illustrates the constitutional limitations applicable to cyber legislation. The Supreme Court invalidated Section 66A of the Information Technology Act on the ground that it violated the constitutional guarantee of freedom of speech and expression.³⁵

4.4 Investigation of Cybercrime Against Women

The effectiveness of cybercrime legislation is strongly influenced by the manner in which complaints are investigated. Unlike many conventional offences, cybercrime investigations often require specialised technical knowledge. Investigators may be required to trace digital accounts, examine devices, obtain relevant platform records, recover deleted information and establish the connection between an individual and specific online activity.³⁶

Victims may also unintentionally compromise evidence because of fear, embarrassment or emotional distress. A woman may immediately block an offender or delete abusive messages without preserving copies. Such actions may sometimes make subsequent investigation more difficult. Consequently, awareness regarding the preservation of digital evidence is important. Where possible, victims should retain screenshots, messages, URLs, account details, emails, photographs, videos and other relevant electronic records before deleting or altering them. Proper preservation of such material can help investigators reconstruct events and establish links between the accused and the alleged conduct.

4.5 Digital Evidence and Its Challenges

Electronic evidence constitutes an essential component of most cybercrime investigations. Unlike physical evidence, digital information can be duplicated, modified, transmitted or deleted within a very short period. Establishing its authenticity, reliability and integrity is therefore crucial.

For instance, screenshots of threatening messages in a cyberstalking case may initially indicate the occurrence of an offence. Investigators may nevertheless need additional technical information to establish the origin of the communication and identify the person responsible.

³⁵ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1. The Supreme Court declared Section 66A of the Information Technology Act, 2000 unconstitutional for violating Article 19(1)(a) of the Constitution.

³⁶ United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 7: Cybercrime Investigation*, discussing the technical requirements involved in the identification, collection and examination of digital evidence.

Likewise, cases involving deepfake material may require specialised examination to determine whether an image, video or audio recording has been manipulated.

The enormous quantity of digital information generated during cybercrime investigations also creates practical difficulties. Police authorities may have to examine extensive collections of messages, images, videos, files and other electronic records. Consequently, sufficient forensic infrastructure, technical resources and appropriately trained personnel are necessary for the effective examination of digital evidence.³⁷

4.6 Jurisdictional Challenges

Cybercrime often extends beyond traditional geographical boundaries. The offender may be situated in one State, the victim in another, while the relevant electronic data may be stored on servers located in a different country. Such circumstances create considerable difficulties in determining and exercising jurisdiction.

Traditional territorial concepts are not always readily applicable to cyber offences because digital communications can cross multiple geographical boundaries almost instantaneously. Investigators may also require information from foreign technology companies or governmental authorities to establish the identity of an offender.

Cross-border investigations can consequently be time-consuming. Such delays are particularly serious where intimate images, threats or continuing harassment are involved, as harmful content may remain accessible or continue to circulate during the investigation. International cooperation, mutual legal assistance and coordination among law enforcement agencies are therefore important for effective investigation and prosecution.³⁸

4.7 Critical Assessment of Enforcement Mechanisms

The Indian framework possesses several significant strengths. It incorporates multiple statutory provisions, national cybercrime reporting mechanisms, specialised investigative units and constitutional safeguards relating to privacy and dignity. The interaction between cyber-specific legislation and general criminal law also enables authorities to respond to a wide variety of technology-facilitated offences.

Despite these strengths, effective enforcement remains a substantial concern. The practical operation of the law depends upon adequately trained police personnel, skilled cyber-forensic

³⁷ Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), provisions relating to electronic and digital records; United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 7: Cybercrime Investigation*.

³⁸ UNODC, *Cybercrime Module 5: Cybercrime Investigation and International Cooperation*, discussing the transnational nature of cybercrime and the importance of international cooperation and mutual legal assistance

experts, suitable technological infrastructure, cooperation from online platforms and timely judicial intervention. This may result in a gap between the law as formally enacted and its implementation in practice.³⁹

Accordingly, strengthening enforcement and institutional capacity is as important as introducing new legislation. The effectiveness of cybercrime regulation ultimately depends not only upon the existence of legal provisions but also upon their consistent and timely implementation.

CHAPTER V

SUGGESTIONS AND CONCLUSION

5.1 Introduction

The present research, entitled **“A Critical Study on Cybercrime Laws for Protection of Women,”** has analysed the legal and institutional measures existing in India for safeguarding women from cybercrime. The study has examined the evolving character of cyber offences, the various forms of technology-enabled crimes affecting women, the constitutional and statutory protections available to victims, and the functions performed by law enforcement authorities and the judiciary. It has also considered the difficulties associated with digital evidence and cyber forensics, together with the emerging risks posed by artificial intelligence and deepfake technology.

The research has primarily followed a doctrinal, analytical and comparative approach. Constitutional provisions, statutory enactments, judicial decisions, legal writings, government sources and institutional mechanisms have been examined as part of the study. The findings indicate that India possesses a considerable legal framework for dealing with cybercrime. However, the practical effectiveness of these laws is largely dependent upon their implementation, technological resources, institutional coordination and the ability of victims to obtain accessible and timely remedies.⁴⁰

5.2 Overall Analysis of the Study

5.2.1 Cybercrime Against Women is a Growing Legal Concern

The study establishes that the widespread use of smartphones, social media, digital

³⁹ Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; and Government of India, National Cyber Crime Reporting Portal.

⁴⁰ Constitution of India; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; and Digital Personal Data Protection Act, 2023.

communication and online services has created additional avenues for offences against women. Cybercrime may occur in various forms, including cyberstalking, cyberbullying, online sexual harassment, cyber defamation, identity theft, impersonation, sextortion, non-consensual dissemination of intimate images, morphing, doxxing and online blackmail. The development of artificial intelligence has further increased the potential for abuse through manipulated photographs, deepfake videos and synthetic media.

5.2.2 Cybercrime Has Consequences Beyond the Digital Environment

The findings demonstrate that cybercrime against women cannot be viewed solely as a technological or criminal-law issue. Its effects may extend to the victim's mental well-being, dignity, privacy, reputation, relationships, education, employment and financial security. Digital material can be reproduced and redistributed repeatedly, thereby prolonging the harm caused by the original offence. Even after the removal of harmful content, victims may continue to experience fear, anxiety and a sense of insecurity.

5.2.3 India Has a Multi-Layered Legal Framework

The study finds that India has developed a layered system of legal protection consisting of constitutional safeguards and multiple statutory enactments. Constitutional provisions protect important interests such as equality, liberty, dignity and privacy. The Information Technology Act, 2000 contains provisions addressing various cyber-related offences, while the Bharatiya Nyaya Sanhita, 2023 contains substantive criminal provisions that may apply to conduct carried out through digital platforms. The Bharatiya Nagarik Suraksha Sanhita, 2023 establishes the procedural framework governing criminal investigation and proceedings, whereas the Bharatiya Sakshya Adhiniyam, 2023 provides the evidentiary framework relevant to electronic and digital material. The Digital Personal Data Protection Act, 2023 further contributes to the legal framework concerning the processing and protection of personal data.⁴¹

5.2.4 Existing Laws Can Address Several Forms of Cybercrime

The research indicates that existing Indian legislation can be invoked in relation to numerous forms of cybercrime against women. Depending on the circumstances of a particular case, provisions dealing with identity theft, personation, privacy violations, sexually explicit electronic material, stalking, sexual harassment, criminal intimidation and defamation may provide appropriate legal remedies.

⁴¹ Constitution of India, arts. 14, 19 and 21; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023; Digital Personal Data Protection Act, 2023.

5.2.5 Technological Development Creates Legislative Challenges

A significant finding of the study is that technological progress frequently takes place at a faster pace than legislative reform. New forms of digital abuse may emerge before specific legal provisions are introduced to address them. Artificial intelligence and deepfake technology provide notable examples of this problem.⁴²

Although existing legal provisions may be capable of addressing particular aspects of AI-generated or manipulated content, there may be a need for clearer and more comprehensive legal provisions dealing specifically with the various forms of technology-enabled abuse directed against women.

5.2.6 Digital Evidence is Central to Cybercrime Prosecution

The study establishes that electronic evidence frequently forms the foundation of cybercrime investigations and prosecutions. Emails, messages, photographs, videos, social media records, electronic transactions and other digital records may be crucial for establishing the occurrence of an offence and connecting the accused with the conduct. At the same time, digital material is particularly vulnerable to deletion, alteration, duplication and manipulation. It is therefore necessary to ensure its proper collection, preservation, authentication and forensic examination so that it can be reliably presented before the court.

5.2.7 Cyber-Forensic Capacity Requires Strengthening

The research finds that effective investigation of cyber offences requires adequate cyber-forensic facilities and appropriately trained personnel. Investigating authorities may need to examine electronic devices, retrieve deleted information, identify fraudulent accounts, analyse manipulated photographs and videos, and trace online activity. Where technical expertise, forensic laboratories or suitable technological resources are inadequate, the ability of investigating agencies to identify offenders and establish the necessary evidence may be adversely affected.

5.2.8 Underreporting Remains a Significant Problem

The study identifies underreporting as an important obstacle to understanding and addressing cybercrime against women. Victims may avoid approaching authorities because of fear, embarrassment, social stigma, family pressure, inadequate awareness of legal remedies or concerns regarding the confidentiality of their personal information. This creates a disparity between the actual incidence of cybercrime and the number of cases formally reported.

⁴² United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 2: General Types of Cybercrime*, discussing the evolving nature of cybercrime and challenges created by emerging technologies.

Underreporting also limits the ability of government authorities and policymakers to determine the true magnitude and changing patterns of cybercrime against women.⁴³

5.3 Suggestions and Recommendations

5.3.1 Strengthening the Legal Framework

Cybercrime legislation should undergo continuous evaluation so that it remains capable of responding to technological changes. Emerging offences, particularly those involving AI-generated images, deepfakes and synthetic media, require appropriate and clearly defined legal treatment. Any legislative development should provide effective protection and remedies to victims while respecting constitutional guarantees and avoiding disproportionate restrictions upon legitimate online expression.⁴⁴

5.3.2 Specific Measures Against Deepfake Abuse

Greater legal and institutional attention should be directed towards AI-generated sexual, defamatory and otherwise harmful content targeting women. Clear mechanisms should be established for reporting, verifying and removing manipulated material. Victims should be provided with rapid avenues for requesting the removal of unlawful content. At the same time, investigating agencies should have access to appropriate technological and forensic tools capable of detecting and analysing manipulated digital material.⁴⁵

5.3.3 Strengthening Cyber-Forensic Infrastructure

Cyber-forensic laboratories should be equipped with modern technological facilities and supported by adequately trained experts. Police and investigating officers should receive regular training in digital evidence, social media investigations, artificial intelligence, deepfake detection and other emerging forms of technology. Improving forensic capabilities would enhance the ability of authorities to trace offenders, recover relevant information and present reliable evidence before judicial authorities.⁴⁶

5.3.4 Simplifying the Reporting Process

⁴³ Government of India, Ministry of Home Affairs, *National Cyber Crime Reporting Portal*; UN Women, materials concerning barriers to reporting and victim support in cases of online and ICT-facilitated violence against women and girls.

⁴⁴ *Constitution of India*, arts. 14, 19 and 21; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023.

⁴⁵ Information Technology Act, 2000, particularly §§ 66E, 67 and 67A; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, concerning unlawful online content, intermediary obligations and grievance redressal.

⁴⁶ Bharatiya Sakshya Adhiniyam, 2023, provisions concerning electronic and digital records; UNODC, *Cybercrime Module 7: Cybercrime Investigation*, concerning digital investigation and forensic examination of electronic evidence.

Cybercrime complaint procedures should be made straightforward, accessible and user-friendly. Women should be able to report cyber offences without encountering unnecessary procedural or technological barriers. Information concerning available legal remedies and reporting channels should be communicated in clear language and, wherever feasible, made available in regional languages to improve accessibility.⁴⁷

5.3.5 Improving Victim Privacy

The confidentiality and personal information of women victims should be protected throughout the investigative and judicial processes. Sensitive photographs, videos, communications and other personal records must be handled through secure procedures. Unnecessary disclosure of such information should be avoided in order to prevent further exposure, humiliation or secondary victimisation of the complainant.

5.3.6 Digital Literacy Programmes for Women

Government bodies, educational institutions and civil society organisations should develop digital literacy initiatives aimed specifically at improving women's online safety. Such programmes should provide practical information concerning account security, privacy settings, online consent, safe communication, cybercrime reporting procedures and preservation of electronic evidence. Greater awareness can empower women to identify risks and respond promptly when cyber abuse occurs.⁴⁸

5.4 Conclusion

Cybercrime against women has emerged as a significant legal and social concern in the contemporary digital environment. The expansion of social media, smartphones, online communication and artificial intelligence has created additional avenues for social and economic participation, while simultaneously producing new forms of vulnerability. The study demonstrates that India has established a substantial legal and institutional framework for addressing cybercrime against women. Constitutional guarantees relating to equality, dignity, privacy and personal liberty form an important foundation for such protection. These safeguards are supplemented by the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Digital Personal Data Protection Act, 2023. Nevertheless, the

⁴⁷ Government of India, Ministry of Home Affairs, *National Cyber Crime Reporting Portal*, providing an online mechanism for reporting cybercrime and improving accessibility to cybercrime complaint procedures.

⁴⁸ Government of India, Ministry of Home Affairs, *National Cyber Crime Reporting Portal*, concerning cybercrime reporting and public awareness; UN Women, resources concerning women's online safety and prevention of technology-facilitated violence.

findings make it clear that legislation by itself cannot guarantee effective protection. The practical success of the legal framework depends upon effective implementation, adequately trained investigators, modern cyber-forensic facilities, reliable mechanisms for handling digital evidence, timely judicial intervention, cooperation from online platforms and accessible support services for victims.

The rapid advancement of artificial intelligence presents one of the most significant challenges for the future. Deepfakes and synthetic media have increased the possibilities of sexual exploitation, impersonation, reputational damage and invasion of privacy. The legal system must consequently develop the capacity to respond to these technologies while continuing to respect constitutional rights, due process and legitimate freedom of expression.⁴⁹

The study therefore concludes that India's existing legal framework provides a strong foundation, but continuous improvement is necessary to address emerging forms of cybercrime effectively. Legislative development must be accompanied by stronger enforcement, improved cyber-forensic capabilities, digital literacy, platform accountability, victim protection, rehabilitation, appropriate compensation and international cooperation.

Ultimately, safeguarding women in cyberspace requires more than merely criminalising harmful conduct. It requires a justice system that is accessible, technologically equipped, victim-oriented, constitutionally balanced and capable of adapting to emerging forms of cybercrime. Strengthening these dimensions can contribute towards creating a safer digital environment in which women can participate in online spaces with greater security, dignity and confidence.

WHITE BLACK **ACTS AND STATUTES**

The Constitution of India, arts. 14, 15, 19 and 21 (Legislative Department, Ministry of Law and Justice, Government of India).

The Information Technology Act, 2000 (Act No. 21 of 2000), especially §§ 43, 66, 66C, 66D, 66E, 67, 67A, 67B and 67C.

The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).

The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).

The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).

The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

⁴⁹ UNODC, *Cybercrime Module 2: General Types of Cybercrime*, concerning emerging and technology-enabled forms of cybercrime; Information Technology Act, 2000, particularly §§66E, 67 and 67A, concerning privacy violations and obscene or sexually explicit electronic material.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.

BIBLIOGRAPHY

Aparna Viswanathan, Cyber Law: Indian and International Perspectives.

Pavan Duggal, Cyber Law: The Indian Perspective.

Yatindra Singh, Cyber Laws.

Jagadhish Raju B. & V. Karthikeyan, A Study on Legal Framework Governing Cyber Crimes Against Women in India (2026).

Priyanka Sethi, Bharatiya Nyaya Sanhita 2023: A Critical Analysis of Legal Reforms in Sexual Offences and Women's Rights in India (2025).

WEBLIOGRAPHY

India Code, Legislative Department, Ministry of Law and Justice, Government of India — <https://www.indiacode.nic.in/>

Legislative Department, Ministry of Law and Justice, Government of India — Constitution of India — <https://legislative.gov.in/>

Ministry of Electronics and Information Technology, Government of India — Digital Personal Data Protection Act, 2023 — <https://www.meity.gov.in/content/digital-personal-dataprotection-act-2023>

National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India — <https://www.cybercrime.gov.in/>

National Crime Records Bureau, Government of India — <https://www.ncrb.gov.in/>

UNODC SHERLOC — Cybercrime Module Series — <https://sherloc.unodc.org/>

Supreme Court of India — <https://www.sci.gov.in/>