Social media crimes against women: Examining legal remedies and enforcement mechanisms in India

Ashish[1]*, Dr. Mani Kumar Meena[2]

[1] Research Scholar, Jaipur School of Law Maharaj Vinayak Global University, Jaipur, Rajasthan

askkne@gmail.com

[2] Supervisor, Jaipur School of Law Maharaj Vinayak Global University, Jaipur, Rajasthan

Abstract

The rapid expansion of digital communication technologies and social media platforms has transformed the manner in which individuals interact, communicate, and participate in public discourse. While social media has created opportunities for empowerment, education, economic participation, and freedom of expression, it has simultaneously emerged as a platform for gender-based cyber violence and online exploitation against women. In India, the increasing penetration of smartphones, internet accessibility, and social networking applications has significantly increased incidents of cyber stalking, online harassment, cyber bullying, identity theft, revenge pornography, morphing of images, impersonation, sextortion, trolling, deepfake exploitation, and non-consensual circulation of intimate content targeting women. These forms of digital abuse not only violate the dignity, privacy, and autonomy of women but also create severe psychological, emotional, social, and economic consequences.

The present article critically examines the growing nature of social media crimes against women in India and analyses the adequacy of the legal remedies and enforcement mechanisms available under Indian law. The study explores constitutional protections, provisions of the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, and other relevant legal frameworks aimed at protecting women from cyber victimization. The article also examines judicial trends, landmark case laws, cyber policing initiatives, role of cyber cells, digital forensic mechanisms, and institutional challenges faced in investigation and prosecution of cyber offences against women.

The article further highlights socio-legal challenges including underreporting of cyber crimes, lack of awareness, victim blaming, jurisdictional complexities, anonymity of offenders, technological advancements, misuse of artificial intelligence, and inadequate digital literacy among users. The study emphasizes the necessity of strengthening cyber governance, digital awareness, gender-sensitive policing, victim support systems, and international cooperation to effectively combat social media crimes against women. The article concludes that although India has established a developing legal and institutional framework to address cybercrimes, stronger implementation, technological preparedness, legal reforms, and coordinated

enforcement mechanisms are essential for ensuring meaningful protection of women in the digital age.

Keywords: Cyber Crime, Women Protection, Social Media, Cyber Harassment, Online Abuse, Cyber Stalking, Digital Violence, Information Technology Act, Gender Justice, Cyber Law.

INTRODUCTION

The emergence of the internet and digital communication technologies has revolutionized social interaction, communication systems, governance, commerce, education, and entertainment across the world. Social media platforms such as Facebook, Instagram, WhatsApp, X (formerly Twitter), YouTube, Telegram, Snapchat, and other digital networking applications have become integral components of modern society. These platforms provide individuals with opportunities for communication, self-expression, professional networking, information sharing, activism, and economic participation. However, the rapid growth of social media has simultaneously contributed to the rise of cybercrimes, particularly gender-based online violence targeting women.

In India, the increasing accessibility of smartphones and internet connectivity has significantly expanded the digital participation of women. Women today actively engage in online education, employment, entrepreneurship, political participation, social interaction, and digital advocacy. Despite these advancements, social media platforms have also become spaces for harassment, intimidation, exploitation, and abuse against women. Cyber offenders frequently misuse digital platforms to commit offences such as cyber stalking, online sexual harassment, revenge pornography, cyber bullying, morphing of images, identity theft, deepfake pornography, impersonation, doxing, blackmail, and dissemination of obscene content. Such crimes not only threaten the safety and dignity of women but also undermine their constitutional rights to privacy, equality, freedom, and dignity.

Social media crimes against women are often characterized by anonymity, rapid dissemination of harmful content, cross-border jurisdictional complexities, and technological sophistication. Unlike conventional crimes, cyber offences can occur continuously and invisibly, making investigation and prosecution difficult for law enforcement agencies. The psychological impact of online victimization is profound, as victims frequently experience trauma, depression, social isolation, reputational harm, anxiety, and fear. In many cases, women

withdraw from online participation due to continuous harassment and digital abuse, thereby affecting their freedom of expression and participation in public discourse.

India has witnessed a significant increase in cybercrimes against women during the last decade. Reports published by the National Crime Records Bureau indicate rising cases of cyber stalking, online fraud, cyber pornography, and social media harassment involving women victims. The COVID-19 pandemic further accelerated online interactions, increasing women's exposure to cyber threats and digital exploitation. The misuse of artificial intelligence, deepfake technologies, and encrypted communication platforms has created new challenges for cyber law enforcement agencies.

Recognizing the growing threat of cybercrimes, India has developed legal frameworks under the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, and related criminal laws to regulate cyber offences and protect victims. Judicial institutions have also expanded constitutional protections relating to privacy, dignity, and online safety. However, practical enforcement remains inadequate due to lack of technical expertise, delays in investigation, underreporting of offences, lack of digital awareness, and insufficient coordination between social media companies and law enforcement authorities.

The present study critically examines the nature and extent of social media crimes against women in India and evaluates the effectiveness of legal remedies and enforcement mechanisms available under Indian law. The article also explores emerging challenges relating to digital governance, cyber policing, victim protection, and technological regulation in the context of women's safety in cyberspace.

Concept and Nature of Social Media Crimes Against Women

Cybercrimes against women refer to unlawful acts committed through digital technologies, internet services, electronic communication systems, and social media platforms with the intention of harassing, intimidating, exploiting, threatening, humiliating, or victimizing women. These offences may be sexual, psychological, emotional, financial, or reputational in nature and are often facilitated through anonymity and technological tools. Social media crimes against women may take various forms including:

- Cyber stalking

- Online sexual harassment
- Revenge pornography
- Cyber bullying
- Identity theft and impersonation
- Deepfake pornography
- Morphing and editing of photographs
- Sextortion
- Doxing
- Online trolling and hate speech
- Non-consensual circulation of intimate content
- Blackmail and extortion
- Defamation through digital platforms
- Financial fraud targeting women

Cyber stalking involves repeated monitoring, communication, or surveillance of women through digital platforms with the intention of causing fear, intimidation, or harassment. Revenge pornography refers to the non-consensual publication or distribution of intimate images or videos of women, often by former partners or acquaintances. Morphing involves editing photographs of women into obscene or sexually explicit images for circulation on social media platforms.

Deepfake technology has emerged as a serious threat in recent years. Artificial intelligence tools can manipulate facial features and voices to create fake pornographic videos involving women. Such content can rapidly spread across digital platforms, causing irreversible reputational and psychological harm.

Online harassment and trolling frequently target women journalists, activists, students, professionals, and political leaders. Misogynistic comments, rape threats, body shaming, and

abusive messages are increasingly common on social media platforms. Women belonging to marginalized communities often face intersectional discrimination based on caste, religion, ethnicity, or political identity. Cybercrimes against women differ from traditional offences because of:

- Anonymity of offenders
- Speed of dissemination
- Global reach of digital platforms
- Difficulty in tracing offenders
- Persistence of harmful content online
- Jurisdictional complications
- Technological sophistication

These offences create long-lasting emotional and social consequences and may severely impact women's mental health, personal relationships, professional opportunities, and social participation.

Constitutional Protection of Women Against Cyber Crimes

The Constitution of India provides the foundational framework for protection of women against online exploitation and cyber violence. Several constitutional provisions are relevant in addressing social media crimes against women.

Article 14: Right to Equality

Article 14 guarantees equality before law and equal protection of laws. Cybercrimes targeting women violate the principle of gender equality by creating discriminatory and hostile digital environments that restrict women's participation in online spaces.

Article 15: Prohibition of Discrimination

Article 15 prohibits discrimination on grounds of sex and permits the State to enact special provisions for women and children. Legal measures relating to cyber protection of women derive constitutional legitimacy from this provision.

Article 19(1)(a): Freedom of Speech and Expression

Women possess the constitutional right to freely express opinions and participate in digital communication. Online harassment and intimidation often suppress women's participation in public discourse and undermine freedom of expression.

Article 21: Right to Life and Personal Liberty

The Supreme Court of India has expanded Article 21 to include:

- Right to privacy
- Right to dignity
- Right to reputation
- Right to mental well-being
- Right to safe environment

Cybercrimes such as revenge pornography, cyber stalking, and online abuse violate these constitutional protections.

In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court recognized privacy as a fundamental right under Article 21, thereby strengthening legal protection against digital surveillance and online exploitation.

Legal Framework Governing Cyber Crimes Against Women in India

Information Technology Act, 2000: The Information Technology Act, 2000 is the primary legislation governing cyber offences in India.

- **Section 66-C (Identity Theft):** Punishes fraudulent use of electronic signatures, passwords, and identity information.
- **Section 66-D (Cheating by Personation):** Punishes impersonation through computer resources and communication devices.
- **Section 66-E (Violation of Privacy):** Punishes capturing, publishing, or transmitting images of private areas of individuals without consent.

- **Section 67:** Punishes publication or transmission of obscene material in electronic form.
- **Section 67-A:** Punishes publication or transmission of sexually explicit material.
- **Section 67-B:** Punishes child pornography and related offences.
- **Section 69-A:** Provides power to block public access to online content threatening public order or security.

Bharatiya Nyaya Sanhita, 2023 and Protection of Women

The Bharatiya Nyaya Sanhita, 2023 contains several provisions relevant to cyber offences against women.

Important offences include:

- Sexual harassment
- Voyeurism
- Stalking
- Criminal intimidation
- Defamation
- Publication of obscene material
- Insulting modesty of women

Cyber stalking through social media communication may attract provisions relating to stalking and criminal intimidation. Circulation of obscene images may attract provisions relating to obscenity and sexual exploitation.

Judicial Approach Towards Cyber Crimes Against Women

Indian judiciary has played a crucial role in protecting women from cyber victimization.

- **Shreya Singhal v. Union of India:** The Supreme Court struck down Section 66A of the IT Act due to unconstitutional restrictions on free speech. However, the judgment also emphasized the need for balanced cyber regulation.
- **State of Tamil Nadu v. Suhas Katti:** One of India's earliest convictions involving cyber harassment and online abuse against a woman.
- **K.S. Puttaswamy v. Union of India:** Strengthened privacy rights in digital spaces.
- Courts have increasingly recognized online abuse as a violation of dignity, privacy, and constitutional freedoms.

Enforcement Mechanisms in India

Cyber Crime Cells

Specialized cybercrime cells have been established across Indian states to investigate digital offences. These units handle:

- Social media complaints
- Financial cyber fraud
- Identity theft
- Online sexual harassment
- Cyber stalking

National Cyber Crime Reporting Portal

The Government of India launched the cybercrime reporting portal for online registration of complaints relating to:

- Women and child cyber abuse
- Revenge pornography
- Social media harassment
- Financial fraud

Digital Forensic Mechanisms

Digital forensic laboratories assist in:

- Recovery of deleted content
- Device analysis
- IP tracing
- Metadata examination
- Evidence preservation

Role of Social Media Platforms

Platforms are increasingly required to:

- Remove unlawful content
- Respond to takedown requests
- Cooperate with law enforcement agencies
- Develop grievance redressal systems

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations upon intermediaries.

Challenges in Enforcement

Despite legal provisions, several practical challenges continue to hinder effective enforcement.

Underreporting: Many women avoid reporting cyber offences due to:

- Social stigma
- Fear of victim blaming
- Lack of confidence in authorities
- Privacy concerns

Technological Challenges: Offenders often use:

- VPN services
- Encrypted communication
- Fake identities
- Foreign servers

Jurisdictional Problems: Cyber offences frequently involve cross-border elements, complicating investigation and prosecution.

Delay in Investigation: Shortage of trained cyber personnel and forensic infrastructure causes delays.

Lack of Digital Literacy: Many users are unaware of:

- Privacy settings
- Reporting mechanisms
- Legal remedies

Misuse of Artificial Intelligence: Deepfakes and AI-generated content create new legal and evidentiary challenges.

Socio-Legal Impact of Social Media Crimes on Women

Cybercrimes have severe consequences on women's:

- Mental health
- Reputation
- Social relationships
- Professional opportunities
- Freedom of expression

Victims often experience:

- Anxiety
- Depression
- Trauma
- Social isolation
- Fear of public participation

Women journalists, activists, politicians, and professionals are disproportionately targeted through coordinated online abuse campaigns.

Cyber victimization may also discourage women from:

- Participating in public discourse
- Using digital platforms
- Engaging in online education and employment opportunities

Thus, cyber violence directly affects gender equality and democratic participation.

Comparative International Perspective

Several countries have enacted strong cyber protection laws for women.

- **United Kingdom:** The UK criminalizes revenge pornography and online harassment under specific legislation.
- **United States:** Various states have enacted laws against cyber stalking and non-consensual pornography.
- **European Union:** The General Data Protection Regulation (GDPR) strengthens digital privacy rights.
- **Australia:** Australia has established eSafety Commissioners for online safety enforcement.

India may adopt comparative best practices including:

- Faster takedown procedures

- Specialized victim support
- AI regulation
- Platform accountability

Suggestions and Recommendations

1. India should enact comprehensive legislation specifically addressing gender-based cyber violence.
2. Cyber police units should be strengthened with trained personnel and digital forensic infrastructure.
3. Awareness campaigns relating to cyber safety and digital literacy should be conducted among women and students.
4. Social media platforms must establish rapid grievance redressal and content removal mechanisms.
5. Educational institutions should include cyber safety education in academic curricula.
6. Victim counselling and psychological support mechanisms should be expanded.
7. International cooperation should be strengthened for cross-border cyber investigations.
8. Artificial intelligence and deepfake technologies should be regulated through specific legal frameworks.
9. Fast-track cyber courts may be established for speedy disposal of cases involving women victims.
10. Gender-sensitive training should be provided to police officers and investigators.

CONCLUSION

Social media crimes against women represent one of the most serious challenges emerging in the digital age. Although technology has empowered women by enhancing communication, participation, and access to opportunities, it has simultaneously exposed them to new forms of exploitation, harassment, and cyber violence. Cyber stalking, revenge pornography, trolling,

online harassment, deepfake exploitation, and non-consensual dissemination of intimate content have become increasingly common in India's digital landscape.

India has developed a growing legal framework through the Information Technology Act, criminal laws, constitutional jurisprudence, intermediary regulations, and cyber policing initiatives. Judicial recognition of privacy, dignity, and digital rights has strengthened women's legal protection in cyberspace. However, enforcement challenges including underreporting, lack of awareness, technological complexities, jurisdictional issues, and inadequate institutional capacity continue to undermine effective implementation.

The increasing misuse of artificial intelligence and anonymous digital technologies further complicates cyber governance and victim protection. Therefore, India requires stronger legislative reforms, gender-sensitive enforcement mechanisms, technological preparedness, victim support systems, and public awareness initiatives to effectively combat cyber crimes against women.

A holistic and coordinated approach involving lawmakers, judiciary, law enforcement agencies, educational institutions, civil society organizations, technology companies, and citizens is essential for ensuring safe and inclusive digital spaces for women. Protection of women in cyberspace is not merely a legal necessity but a constitutional and social obligation essential for preserving dignity, equality, privacy, and democratic participation in the digital era.

References

1. Agarwal, H. (2022). *Cyber law and crimes in India*. Allahabad Law Agency.

2. Bansal, A. (2021). Cyber violence against women in India: Emerging legal concerns. *Indian Journal of Law and Justice*, *12*(2), 45–61.

3. Bharatiya Nagarik Suraksha Sanhita, 2023.

4. Bharatiya Nyaya Sanhita, 2023.

5. Bharatiya Sakshya Adhiniyam, 2023.

6. Duggal, P. (2020). *Cyber law in India*. Saakshar Law Publications.

7. Government of India. (2000). *Information Technology Act, 2000*.

8. Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

9. Halder, D., & Jaishankar, K. (2017). *Cybercrimes against women in India*. Sage Publications.

10. Jain, M. P. (2022). *Indian constitutional law* (9th ed.). LexisNexis.

11. Kaur, A. (2023). Social media harassment and women's safety in India. *Journal of Cyber Law Studies, 8*(1), 77–95.

12. Kumar, V. (2021). Cyber stalking and digital abuse against women: Legal challenges in India. *Indian Bar Review, 48*(3), 102–118.

13. National Crime Records Bureau. (2024). *Crime in India Report 2023*. Ministry of Home Affairs.

14. Puttaswamy v. Union of India, (2017) 10 SCC 1.

15. Sharma, R. (2022). Deepfake technology and cyber exploitation of women in India. *International Journal of Digital Law, 5*(2), 56–74.

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

17. Singh, P. (2021). Gender-based cyber violence and legal responses in India. *Journal of Human Rights and Gender Justice, 6*(1), 34–52.

18. State of Tamil Nadu v. Suhas Katti, C.C. No. 4680/2004.

19. United Nations. (2020). *Cyber violence against women and girls: A global wake-up call*. UN Women.

20. Verma, S. (2023). Legal regulation of social media crimes in India. *Journal of Information Technology and Law, 11*(2), 88–109.

21. World Health Organization. (2021). *Violence against women in digital spaces*. WHO Publications.

22. Yadav, N. (2022). Online gender-based violence in India: Legal and policy perspectives. *Indian Journal of Social Legal Studies, 4*(1), 66–84.

23. Zuboff, S. (2019). *The age of surveillance capitalism*. Public Affairs.

24. Ministry of Home Affairs. (2023). *National cybercrime reporting portal guidelines*. Government of India.

25. United Nations Office on Drugs and Crime. (2022). *Cybercrime and gender-based violence*. UNODC Publications.