Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 1539–1544

CYBER CRIMES AGAINST WOMEN IN INDIA

Himani Ahlawat, Dr. Somlata Sharma

[1] Research Scholar, MDU-CPAS, Gurugram
[2] Associate Professor, MDU-CPAS, Gurugram

DOI
10.29121/shodhkosh.v5.i6.2024.2430

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The fast growth of technology and extensive internet usage have resulted in an alarming increase in cybercrime, particularly targeting women. In India, where women already face enough obstacles in the physical world, the internet domain has become yet another source of harassment and abuse. This study investigates the many types of cybercrimes committed against women in India, their socio-legal ramifications, and legislative and judicial reactions to these crimes. It also investigates the effects of such crimes on women's mental health, freedom of expression, and overall involvement in the digital economy. This study uses case studies and statistical analysis to expose weaknesses in existing regulations and propose remedies to tackle this growing threat.

Keywords: Cybercrimes, Women, IT ACT, Internet, Cyberlaw

1. INTRODUCTION

The fast spread of the internet and digital technologies has altered how we communicate, interact, and engage with the world. However, the digital revolution has opened the door to new forms of crime, including cybercrime, which disproportionately affects vulnerable groups, including women. In India, where societal systems frequently impose gendered hierarchies, the virtual world has become yet another arena where women encounter an overwhelming number of risks, ranging from cyberstalking and online harassment to the non-consensual publication of private photographs and gender-based trolling. Cybercrime against women in India has been increasing at an alarming rate, fuelled by factors such as anonymity, widespread smartphone use, and a lack of strict enforcement measures. According to the National Crime Records Bureau (NCRB), cybercrimes against women, such as online harassment, stalking, and defamation, have increased significantly in recent years.[1] The very characteristics that make the internet a platform for free expression—its broad reach, anonymity, and speed—have also made it a breeding ground for abuse and exploitation.

At the heart of this digital threat is the gendered form of cyber assault. While cybercrime affects all users, women are especially vulnerable to kinds of abuse that reflect patriarchal and misogynistic standards seen in the offline world. In

[1] National Crime Records Bureau. (2021). *Crime in India 2021 - Statistics*. Available at: https://ncrb.gov.in/en/crime-india

many circumstances, women's prominence in public and professional settings leads to heightened scrutiny and antagonism online. Acts such as revenge pornography, sexual harassment via messaging systems, and insulting comments on social media are becoming more common. The psychological, social, and professional consequences of such crimes frequently leave victims vulnerable, with little options due to loopholes in the legal framework and the slow pace of justice in the Indian judicial system.

The Information Technology Act of 2000 (IT Act), together with pertinent provisions of the Indian Penal Code (IPC), serves as the legal foundation for dealing with cybercrimes in India. Despite this, legal remedies for women victims of cybercrime remain inadequate due to a lack of gender-specific laws, difficulties with enforcement, and gaps in jurisdictional power. More recently, the Bharatiya Nyaya Sanhita (BNS) 2023 was implemented as part of a larger effort to improve India's criminal justice system. The BNS aims to modernise the legal framework and combat contemporary crimes, especially those committed in internet. However, the real execution and efficacy of such legislative amendments have to be determined.

2. TYPES OF CYBER CRIMES AGAINST WOMEN

Crimes against women in cyberspace can be grouped into various categories, each with its own characteristics and consequences:

1.1. Cyberstalking: Cyberstalking is the use of the internet or technological gadgets to stalk or harass women. The stalker monitors the victim's online activity, sends threatening or unwelcome communications, and invades her privacy. Cyberstalking can cause psychological anguish, fear, and disturbance to daily life.

1.2. Online Harassment: Online Harassment: Women routinely get verbal abuse, threats, and sexually explicit communications on social media and other digital forums. This type of harassment frequently leads to victim blaming, which prevents women from reporting these crimes.

1.3. Cyber Pornography: One of the most serious kinds of cybercrime against women is the unauthorised use or publication of pictures or films, particularly those with sexual content. In many circumstances, intimate information is shared without consent, resulting in public humiliation, extortion, and social isolation.

1.4. Cyberbullying and trolling: Trolling is the practice of posting inflammatory or offensive content with the intention of provoking emotional responses. When directed against women, phrase frequently assumes a sexist or misogynistic tone. Women in politics, the media, and activism are specifically targeted.

1.5. Non-Consensual Dissemination of Private Content: This includes revenge porn and morphing, which is when private photographs or videos are altered and posted online without permission. This is designed to discredit or blackmail the victim, which frequently causes considerable emotional distress.

1.6. Phishing and financial fraud: Women are frequently targeted in phishing attempts, where their personal and financial information is compromised. These attacks may have long-term economic consequences for victims.

2. SOCIO-CULTURAL FACTORS CONTRIBUTING TO CYBER CRIMES AGAINST WOMEN

The rise of cybercrime against women in India can be attributed to deeply ingrained cultural and societal norms. Gender inequality, objectification of women, and patriarchal control over women's bodies and choices exist both in the offline and online worlds. Online forums frequently reflect the same misogyny that women suffer in their daily lives, where they are perceived as inferior or undeserving of privacy and respect. Furthermore, the anonymity provided by the internet allows attackers to harass women without fear of instant repercussions. Cultural stigma and fear of social judgement sometimes deter women from reporting such instances, giving criminals an advantage. These crimes frequently have severe psychological implications for the victims, such as worry, depression, and social withdrawal.

3. LEGAL FRAMEWORK OF CYBERCRIMES AGAINST WOMEN IN INDIA

India has made great progress in combating cybercrime through numerous legislation, yet loopholes persist, particularly in crimes against women.

3.1. The Information Technology (IT) Act, 2000: The Information Technology (IT) Act of 2000 is India's fundamental regulation governing cyber activity and combating many sorts of cybercrime, especially those against women. It was enacted to encourage e-commerce, data protection, and privacy, but its scope has steadily evolved to include cybercrime prevention.[2] Some of its key provisions are discussed below[3].

3.1.1. Section 66E (Violation of Privacy) : This clause penalises the unauthorised capture, publication, or transfer of a photograph of a person's private area. It attempts to protect individuals' privacy, particularly that of women, by penalising the unauthorised sharing of intimate photos. Violators face up to three years in prison, a two-lakh rupee fine, or both.

3.1.2. Section 67 (Punishment for Publishing or Transmitting Obscene Material in Electronic Form) :Section 67 criminalises the electronic publication and transmission of obscene material, including pornographic materials. The first conviction carries a maximum sentence of three years in prison and a five lakh rupee fine. For further convictions, imprisonment can be extended to five years, with a fine of up to ten lakh rupees.

3.1.3. Section 67A (Punishment for Publishing or Transmitting Sexually Explicit Material) : Section 67A governs the publication or transmission of sexually explicit content and carries harsher penalties than Section 67. The first conviction can result in up to five years in prison and a fine of up to ten lakh rupees, with successive convictions punishable by up to seven years in prison.

3.1.4. Section 67B (Punishment for Child Pornography): This clause makes it illegal to publish or transmit content depicting minors performing sexually explicit acts. The punishment is comparable to that under Section 67A, but it is especially important in cases of kids being exploited online.

3.2. Critical Analysis of the IT Act 2000

While the IT Act has various provisions targeted at tackling cybercrime against women, significant deficiencies remain:

3.2.1. Lack of Specific Focus on Gender-Based Cyber Crimes: The IT Act lacks a section specifically addressing gender-based cybercrime. It has generic prohibitions about privacy violations and obscene content, but many crimes affecting women, such as revenge pornography or cyberbullying, are not specifically mentioned or addressed.[4]

3.2.2. Vague Terminology and Enforcement Challenges: The IT Act does not explicitly define terms such as "obscene" and "sexually explicit". This allows for subjective interpretations, which can result in inconsistent judgements and the misuse of the law. For example, while Section 66E criminalises the publication of intimate images, the legislation does not address the psychological and social consequences for women.[5]

3.2.3. Poor Enforcement and Awareness: Despite the IT Act's provisions, enforcement remains a big concern. Law enforcement agents are frequently poorly trained in cyber forensics and digital investigations, which

[2] Government of India. (2000). The Information Technology Act, 2000. Ministry of Law, Justice and Company Affairs. Available at: https://legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000

[3] Kaul, V., & Sinha, M. (2020). "Cyber Crimes in India: Legislative and Judicial Response."

[4] Verma, A. (2021). "The Rising Tide of Cyberstalking and Harassment in India: A Gendered Perspective."

[5] Sharma, R. (2019). "Revenge Porn and the Law: A Global and Indian Perspective."

impedes effective policing. Furthermore, victims are frequently unaware of the options accessible to them, resulting in underreporting of cyber-crimes.[6]

3.2.4. Jurisdictional and Global Challenges: Because of their nature, cybercrimes frequently cross national borders. The IT Act's jurisdiction is limited to India, making it difficult to track down criminals outside of India. Global collaboration among law enforcement authorities remains a difficulty, with many cases unresolved.

3.3. Bharatiya Nyaya Sanhita (BNS) 2023

The Bharatiya Nyaya Sanhita (BNS) 2023 is part of India's proposed legal reform, which intends to replace the colonial-era Indian Penal Code and it includes particular measures addressing current crimes, such as cybercrimes.[7] The relevant provisions regarding cyber-crimes against women under BNS 2023 are as follows[8]:

3.3.1. Cyber Harassment and Defamation: The BNS 2023 proposes more specific definitions and harsher penalties for cyber harassment and defamation, which disproportionately harm women. The bill seeks to modernise the legal terminology governing cyberbullying, online stalking, and defamatory statements on social media platforms.

3.3.2. Revenge Porn and Digital Voyeurism: The BNS makes explicit rules for revenge pornography, which is the non-consensual distribution of personal photos or videos. The BNS specifies clear consequences for abusers, including heavy fines and imprisonment if they share such content with the aim to hurt the victim.[9]

3.3.3. Cyberstalking and Doxing: The BNS aims to strengthen protections against cyberstalking and doxing (the act of publicly revealing personal information online in order to harass or threaten someone). Cyberstalking crimes, which were previously covered by IPC Section 354D[10], will now be covered more extensively by the BNS, which includes measures for prompt redressal and victim protection.

4. JUDICIAL TRENDS

4.1. Shreya Singhal v. Union of India[11] : This landmark case questioned the legitimacy of Section 66A of the Information Technology Act of 2000, which authorised the arrest of persons for posting "offensive" content online. The Supreme Court declared Section 66A illegal because it breached Article 19(1)(a) of the Indian Constitution, which guarantees free speech. Although the case did not explicitly address cybercrime against women, it is significant since Section 66A was frequently utilised to combat online abuse, particularly that of women.

4.2. Kirti Vashisht v. State of Delhi[12]: In this case, the petitioner, Kirti Vashisht, was a victim of revenge porn after her former lover shared intimate images and videos of her online. The accused was charged under Sections 67 and 67A of the Information Technology Act of 2000 (penalty for publishing or distributing obscene or sexually explicit material online). The court found in favour of the victim, resulting in severe punishment for the criminal.

---

[6] Rana, T. (2021). "An Evaluation of the IT Act's Response to Cyber Violence Against Women."

[7] Ministry of Home Affairs. (2023). *Bharatiya Nyaya Sanhita (BNS) 2023*. Bill introduced in the Parliament of India. Available at: https://www.mha.gov.in/en/BNS2023

[8] Patil, R. (2020). "Analyzing the Impact of Bharatiya Nyaya Sanhita 2023 on Women's Digital Rights."

[9] Singh, P. (2022). "Cyberbullying and Legal Safeguards for Women in India."

[10] Government of India. (1860). *Indian Penal Code*. Available at: https://indiacode.nic.in/bitstream/123456789/4219/1/indian_penal_code_1860.pdf

[11] AIR 2015 SC 1523.

[12] 2019 SCC OnLine Del 11713

4.3. **Sree Surya v. State of Kerala**[13]**:** In this case, a college student filed a complaint after experiencing frequent cyberstalking and online abuse. The accused, who was continually sending threatening and abusive communications to the victim, was charged under Sections 354D of the IPC (stalking) and 66A of the Information Technology Act. The court adopted a firm position and convicted the accused.

4.4. **Sushil Ansal v. State through NCT of Delhi**[14]**:** This case concerned the unauthorised sharing of sexually explicit videos of women via an online pornography website. Sushil Ansal, the accused, was charged with sending and publishing sexually explicit content under Section 67A of the IT Act, as well as voyeurism under Sections 354C and 509 of the IPC. The court affirmed the accused's harsh sentencing, emphasising the importance of remaining vigilant against such acts.

4.5. Kalindi Charan Lenka v. State of Odisha[15]: In this case, the accused was charged with creating fake social media identities for a woman and posting defamatory content about her, resulting in harassment and mental anguish. The case was prosecuted under Sections 67 of the IT Act and 500 of the IPC (defamation). The court found the accused guilty, emphasising the necessity of protecting women from identity theft and defamation online.

5. CHALLENGES IN ADDRESSING CYBER CRIMES AGAINST WOMEN

5.1. Underreporting of crimes: Cultural stigma, victim blaming, and the threat of future harassment frequently dissuade women from reporting cybercrimes. Furthermore, many women are unaware of their legal rights and the options for obtaining justice.[16]

5.2. Lack of digital literacy: Many women, particularly in rural regions, lack digital literacy and knowledge about how to defend themselves online. This increases their vulnerability to cybercrime and limits their ability to respond effectively.[17]

5.3. **Jurisdictional Issues**: Cybercrimes frequently cross national borders, making it difficult to identify culprits and enforce laws. India's legal framework struggles to address the global character of the internet, posing substantial obstacles for investigation and punishment.

5.4. **Inadequate Policing**: India's law enforcement organisations frequently lack the technological competence and resources required to properly investigate and prosecute cybercrimes. This, combined with the sluggish court process, impedes justice for victims.[18]

6. RECOMMENDATION AND CONCLUSION

Addressing cybercrime against women requires a multifaceted approach that includes stronger legal frameworks, improved law enforcement, and widespread education. The IT Act should be amended to cover a greater variety of cybercrimes against women, including provisions for revenge pornography, cyberstalking, and online harassment. Police and judges should be given clearer rules for dealing with cybercrime. Government activities should prioritise promoting digital literacy, particularly among women. Awareness initiatives on cyber safety, privacy settings, and reporting

[13] Kerala High Court. (2022). *Sree Surya v. State of Kerala*, Kerala High Court Case No. 2022.

[14] CRL.M.C. 3276/2021

[15] Crl. Appeal No. 157 of 2018.

[16] Agarwal, S. (2019). "Cyber Crimes Against Women in India: Legal Framework and Challenges." Journal of Law and Social Policy, 12(1), pp. 45-67.

[17] Mehta, K. (2020). "Empowering Women Through Digital Literacy in India." *International Journal of Digital Society*, 9(3), pp. 150-162.

[18] Basu, S. (2017). "Gender and Patriarchy in Cyberspace: An Analysis of Cyber Crimes Against Women in India."

procedures will help women protect themselves online. Law enforcement officers must be trained in cyber forensics and digital investigations. Setting up specialised cybercrime units and fast-track courts can help victims receive justice quickly.

Social media networks and technology businesses should work with law enforcement to make the internet a safer place. This includes improving reporting channels, taking prompt action against criminals, and preserving victims' privacy.

Cybercrime against women in India is a growing concern that requires immediate action from policymakers, law enforcement, and society as a whole. While there have been significant judicial and legislative developments, the current legal system falls short of fully safeguarding women from online harassment. Addressing this issue necessitates not just legal changes, but also a cultural shift in attitudes towards women and their right to safety and dignity in cyberspace.

ACKNOWLEDGEMENTS

Authors are thankful to the healthcare practitioners working in GMC, Srinagar who helped directly or indirectly in the collection of data during the field work.

CONFLICT OF INTEREST

The authors declare no conflict of interest between them.