



Cyber Crime Against Women in Indian Context: An Overview

Mohit Bhuriya, Jayshri Nandeshwer
Student, Professor
Sage University Indore

1. Abstract

This research provides a comprehensive overview of cyber crimes targeting women in India. With increased internet penetration and digital services usage, Indian women have become disproportionately vulnerable to various cyber threats. These threats range from cyberbullying, cyberstalking, online harassment, image-based abuse, to identity theft and financial fraud. The study examines the sociocultural, technological, and legal dimensions influencing these crimes. It also evaluates the existing legal framework, including the Indian Penal Code (IPC) and the Information Technology Act, and their effectiveness in addressing digital offenses against women. Through statistical analysis, case studies, and in-depth discussion on preventive and remedial measures, the paper highlights the gaps and challenges in combating cyber crimes. It emphasizes the role of law enforcement agencies, civil society, and technology platforms in strengthening cyber safety for women. Based on empirical evidence and comparative perspectives, the research proposes policy recommendations aimed at fostering better legal enforcement, digital literacy, and women-centric cyber safety initiatives. The study concludes by urging collaborative efforts to build a safer digital ecosystem where women can participate freely without fear of abuse or exploitation.

2. Introduction

Cyber crime against women refers to online harassment, exploitation, or violence targeting women, often through social media, emails, or messaging apps. This can include stalking, bullying, non-consensual sharing of intimate images, online trolling, and more

3. Background

The advent of the internet and digital technologies has transformed societies across the world, enabling communication, access to information, and economic opportunities. In India, rapid digitalization has significantly increased internet accessibility among women. As of 2024, India has over 900 million internet users, with a growing number of women connecting online for education, employment, social networking, and commerce. However, the digital sphere has also become a space where crimes against women are increasingly perpetrated.

4. Emergence of Cyber Crime

Cyber crime refers to illegal activities conducted through digital systems, networks, and the internet. While cyber crime affects all demographics, women are particularly vulnerable due to social inequalities, lack of digital literacy, and existing

offline gender-based violence patterns that extend into the online world.

5. Problem Statement

Despite progressive laws and increasing awareness, cyber crimes against women in India continue to rise. Reported incidents of cyberstalking, revenge pornography, online harassment, and identity theft indicate systemic challenges in prevention, reporting, and prosecution. Many women, out of fear, shame, or distrust of authorities, do not report these crimes, further complicating efforts to quantify and address the issue effectively.

6. Objectives of the Study

To analyze the forms and prevalence of cyber crimes against women in India.

To evaluate the legal and institutional mechanisms available for protection and redress. To assess the psychological, social, and economic impact of cyber crimes on women.

To provide recommendations for policy, enforcement, and awareness campaigns

7. Significance of the Study

Understanding how cyber crimes impact women is crucial for developing targeted strategies to enhance women's safety online. This study contributes to academic discourse, informs policy for law enforcement and legislators, and empowers civil society to take action.

8. Types of Cyber Crime Against Women

1. Online Harassment: Abusive messages, threats, or unwanted attention via social media, emails, or messaging apps.
2. Cyber Stalking: Tracking or monitoring someone's online activities without consent.
3. Non-Consensual Sharing of Images: Sharing intimate photos or videos without permission (revenge porn).
4. Online Trolling: Provoking or attacking women online, often through comments or social media posts.
5. Phishing or Scamming: Targeting women with fake schemes or scams, often through emails or social media.
6. Identity Theft: Stealing personal info to impersonate or exploit women online.
7. Online Sex Trafficking: Using the internet to facilitate sex trafficking or exploitation.

09. legal framework

In India, the legal framework addressing cybercrime against women is primarily governed by the Information Technology Act, 2000 (IT Act) and the Indian Penal Code, 1860 (IPC). Key provisions include:

- Section 354A, IPC: Addresses sexual harassment, including online harassment.
- Section 354D, IPC: Covers stalking, including cyberstalking.
- Section 66E, IT Act: Penalizes capturing, publishing, or transmitting images of a private area without consent.
- Section 67, IT Act: Prohibits publishing or transmitting obscene material.
- Section 67A, IT Act: Deals with publishing or transmitting sexually explicit material.

These laws provide protection against online harassment, stalking, and non-consensual sharing of images. Victims can file complaints with the cybercrime cell or local police

10. Law Enforcement Response

In India, law enforcement agencies are taking steps to tackle cybercrime against women. The National Cyber Crime Reporting Portal (NCRP) allows victims to report incidents, and the Indian Cyber Crime Coordination Centre (I4C) coordinates efforts to combat cybercrime. The government has also set up cyber forensic-cum-training laboratories in 33 states/UTs and provided training to over 24,600 law enforcement personnel.

Key initiatives include:

- Cyber Crime Prevention against Women and Children (CCPWC) scheme: Financial assistance is provided to states/UTs for capacity building and setting up cyber forensic laboratories.
- National Cyber Crime Helpline (1930): A 24/7 helpline for reporting cybercrimes.
- Joint Cyber Coordination Teams: Established in key cities to enhance coordination among law enforcement agencies.

Some notable cases include a recent conviction in an Amreli cybercrime case, where a Nigerian woman was sentenced to 7

years imprisonment for cheating a man of Rs 14.09 lakh ^{1 2 3}

11. Cybercrime against women in India

- Underreporting: Victims often hesitate to report due to social stigma, fear of retaliation, or lack of awareness.
- Lack of digital literacy: Many women aren't aware of online safety measures or how to report incidents.
- Anonymity: Cybercriminals often hide behind fake identities, making it hard to track them.
- Jurisdictional issues: Crimes can involve multiple states or countries, complicating investigations.
- Limited resources: Law enforcement agencies face resource constraints, impacting investigation and prosecution.
- Technological advancements: Cybercriminals constantly adapt, making it challenging for law enforcement to keep up.

12. Conclusion

Cybercrime against women is a growing concern in India, with many facing online harassment, stalking, and exploitation. While laws like the IT Act and IPC provide some protection, challenges like underreporting, lack of digital literacy, and jurisdictional issues persist. Strengthening law enforcement, awareness, and support systems is crucial to combat these crimes effectively.

Reference

- 1 Agarwal, A. (2018). Cyber laws in India. LexisNexis.
- 2 Bakshi, P. M. (2021). The Constitution of India. Universal Law Publishing.
- 3 Chaturvedi, R. (2019). Cyber crime and cyber terrorism. Atlantic Publishers.
- 4 Halder, D., & Jaishankar, K. (2016). Cyber crime and the victimization of women: Laws, rights, and regulations. IGI Global.
- Kshetri, N. (2013).
- 4 Cybercrime and cybersecurity in the global South. Palgrave Macmillan.
- 5 Singh, Y. M. (2020). Indian Penal Code. LexisNexis.

