



Increasing Cyber-Crime Against Women

Author: Rimjhim Boruah

Designation: MA in education, Dibrugarh University

Abstract

The rapid growth of digital technology, internet access, and social media has led to an increase in cyber-crime against women. While online platforms offer opportunities for education, employment, and self-expression, they also expose women to various forms of online abuse. Women are commonly targeted through cyber stalking, online harassment, cyber bullying, identity theft, impersonation, image morphing, defamation, and revenge pornography. These crimes violate women's privacy, dignity, and basic human rights.

Cyber-crime has serious psychological and social effects on women. Victims often suffer from fear, stress, anxiety, depression, loss of confidence, and social isolation. In some cases, women withdraw from education or work due to mental trauma. Although India has laws such as the Information Technology Act, 2000 and provisions under the Indian Penal Code, cyber-crime against women continues to rise due to lack of digital awareness, fear of social stigma, poor reporting systems, and weak enforcement. This paper examines the nature, causes, and impact of cyber-crime against women and emphasizes the need for digital literacy, strict law enforcement, and strong support systems to ensure women's safety online.

Keywords: Cyber-crime, women, online harassment, cyber laws, digital safety.

INTRODUCTION

Cyber-crime is the term used to describe illegal activity involving computers, digital devices, and internet-based networks. The use of cyberspace has spread to nearly every facet of human existence due to the quick development of information and communication technology, including social contact, banking, healthcare, education, and governance. Digital technology has increased efficiency and convenience, but it has also opened up new avenues for criminal activity. As a result, cybercrime has become a major worldwide issue that puts people, businesses, and governments at risk.

Cyber-crime against women has become one of the most pressing challenges in the contemporary digital era. The rapid advancement of information and communication technology, along with widespread access to the internet and social media platforms, has transformed the way people communicate, work, and participate in society. Women today actively engage in digital spaces for education, professional growth, entrepreneurship, and social interaction. However, this increased online participation has also exposed them to a wide range of cybercrimes that specifically target women, making cyberspace a site of both empowerment and vulnerability.

Cyber-crime against women refers to unlawful and harmful activities carried out through digital devices, computer networks, or the internet with the intention of harassing, threatening, exploiting, or violating the dignity and privacy of women. Common forms of such crimes include cyber stalking, cyber bullying, online harassment, identity theft, impersonation, image morphing, revenge pornography, non-consensual sharing of intimate images, and financial fraud. These crimes often aim to control, intimidate, or shame women, reflecting deep-rooted gender biases and power imbalances present in society.

In countries like India, the rise in cybercrime against women has prompted legal and institutional responses, including provisions under the Information Technology Act, 2000, and relevant sections of the Indian Penal Code. Despite these measures, challenges such as lack of awareness, inadequate reporting mechanisms, insufficient training of law enforcement agencies, and delays in the justice system continue to hinder effective prevention and redressal. This highlights the need for stronger enforcement, victim-friendly reporting systems, and gender-sensitive cyber laws.

Literature review

Expanding on emerging technologies, Henry and Powell (2018) argue that digital technologies have transformed gender-based violence, making abuse more persistent and difficult to escape. Their work highlights the growing misuse of technology to monitor, threaten, and humiliate women.

A global perspective is provided by UN Women (2020), which reports that online violence against women has increased worldwide, particularly against women journalists, activists, and politicians. The report emphasizes the need for coordinated legal, technological, and educational interventions.

A comparative legal study by Patil (2021), highlights that India lags behind international conventions such as the Budapest Convention on Cybercrime in providing comprehensive protection to women. The study calls for stronger policy coordination and victim-centric legal reforms.

Farhana (2022), emphasizes that cybercrime against women includes cyber stalking, cyber harassment, online defamation, identity theft, and non-consensual sharing of intimate images. The study highlights that anonymity in cyberspace empowers offenders while social stigma discourages women from reporting such crimes, leading to underestimation of the problem.

Beevi and Ramesh (2023), critically analyze India's legal framework for addressing cybercrime against women. While laws such as the Information Technology Act, 2000 and sections of the Indian Penal Code exist, the authors argue that enforcement remains weak due to lack of trained cyber police units and gender-sensitive procedures.

Ahlawat and Sharma (2024), examine cyber-crime trends in India and find a direct relationship between increased internet penetration and crimes against women online. Their study notes that lack of cyber awareness, weak digital literacy, and limited legal knowledge among women intensify their vulnerability.

Methodology

This is a qualitative study is based on secondary sources of information. The current study is grounded on reviews of the related literature, for which information was gathered from variety of journals, magazines, and websites and published articles that deal with the subject matter.

(a) Data Collection: Relevant data was collected through a systematic review of existing literature, official statistics, and published reports. Emphasis was placed on recent data to reflect current trends in cyber-crime against women.

(b) Data Selection: Reviewing the collected articles which are recently published and relevant to that research topic.

(c) Thematic Analysis: Reading through the selected articles to gain a comprehensive understanding of the challenges highlighted and using coding system to label and categorize challenges based on themes that appear from the articles.

No primary data was collected. Data reliability ensured through cross verification of multiple academic and government sources

Types of cyber-crime against women

1. Cyber Stalking:

Cyber stalking is the repeated use of online platforms to harass or intimidate women. It can include sending threatening messages, monitoring social media activity, or tracking online presence. This often causes fear, anxiety, and disruption in daily life.

2. Online Harassment & Cyber Bullying:

Women can face abusive comments, trolling, and threats on social media or messaging apps. Cyber bullying may target personal appearance, opinions, or professional life. Such harassment leads to emotional distress, social withdrawal, and loss of confidence.

3. Image Morphing:

Morphing involves digitally altering women's images into offensive or sexual content without their consent. These altered images are then shared online to humiliate or intimidate. This constitutes a serious violation of privacy and dignity.

4. Revenge Pornography:

Revenge pornography occurs when private intimate images or videos are shared online without consent. Usually, it is done by ex-partners or people seeking revenge. The act can cause severe emotional trauma and social stigma.

5. Identity Theft & Impersonation:

Cyber criminals may steal personal details or social media profiles of women. They use this information to create fake accounts or commit fraud. Impersonation can damage reputation and may lead to financial or legal issues.

6. Cyber Defamation:

False statements, rumors, or doctored content about women can be posted online to tarnish their reputation. Cyber defamation can spread rapidly and affect personal and professional life. Victims often face social humiliation and mental stress.

7. Phishing & Email Scams:

Women can be targeted through emails or messages that appear trustworthy but are designed to steal personal information. Attackers may seek passwords, banking details, or private data. Falling victim can result in financial loss and identity compromise.

8. Cyber Blackmail & Extortion:

Criminals threaten to release private images or information unless victims meet their demands. The demands may involve money, favors, or silence. This form of crime causes fear, stress, and reputational harm.

Cause of cyber-crime against women

1. More Use of Social Media:

Women use social media for chatting, sharing photos, study, and work. Sometimes they share personal details like photos or location. Cyber criminals misuse this information to harass or threaten them.

2. Lack of Knowledge about Online Safety:

Many women do not know how to use privacy settings or protect passwords. They may click on unknown links or talk to fake profiles. Cyber criminals take advantage of this. This can lead to hacking, cheating, or blackmail.

3. Male Dominated Thinking:

Some people believe women should stay silent or obey. This thinking leads to online abuse against women.

4. Weak Law Enforcement:

Cyber laws exist, but they are not always properly followed. Police may take time to solve cyber cases. Many women lose hope and do not complain.

5. Fear of Society and Shame:

Many women feel ashamed to report cyber-crime. They fear being blamed by society or family. Some think reporting will spoil their image. Because of this, criminals go free.

6. Personal Revenge:

After breakups or arguments, some people try to take revenge online. They share private photos or messages. This is done to hurt and insult women. Revenge cyber-crime is common today.

Impact of cyber-crime on women

1. Psychological Impact:

Cyber-crimes badly affect the mental health of women. Victims often feel fear, stress, anxiety, and sadness. Continuous online harassment makes women feel unsafe even in their own homes.

2. Social Impact:

Cyber-crimes harm the social image and respect of women. Due to shame and fear, victims often stop using social media and avoid social gatherings. They may feel isolated and lonely. This reduces their participation in public and social life.

3. Economic Impact:

Online harassment at the workplace can affect job performance and promotions. Many women stop using online platforms for business or work. This limits their financial growth and independence.

4. Impact on Education and Career:

Female students face cyber bullying and online threats, which disturb their studies. Fear of online abuse reduces concentration and learning ability. Some students stop attending online classes or using digital learning tools.

5. Legal and Reporting Problems:

Many women do not report cyber-crimes due to fear and lack of awareness. They may not know where or how to file a complaint. Long legal procedures discourage victims from seeking justice.

6. Impact on Digital Freedom:

Cyber-crimes restrict women's freedom on the internet. Many women avoid sharing opinions or photos online. They limit their digital presence to protect themselves. This reduces women's voices in online discussions.

7. Family and Emotional Impact

Cyber-crimes also affect women's family life. Some families react negatively and blame the victim. Lack of family support increases emotional pain and helplessness.

Legal framework for cyber-crime against women

1. Constitutional Protection to Women in Cyberspace:

Article 14: Equal protection under the law and equality before the law are guaranteed. **Article 15(1)** and **(3):** Discrimination is prohibited and special accommodations for women are permitted under.

Article 19(1)(a): Freedom of speech, subject to reasonable restrictions on obscenity and defamation.

Article 21: Right to life and personal liberty, interpreted to include right to privacy, dignity, and reputation, which are frequently violated in cyber-crime against women.

2. Information Technology Act, 2000 – Detailed Analysis:

Key Sections Protecting Women:

Section 66C: Punishes identity theft, commonly used in online impersonation of women.

Section 66D: Cheating by personation using computer resources (fake profiles, matrimonial fraud).

Section 66E: Violation of privacy by publishing intimate images without consent.

Section 67: Online publication of obscene content.

Section 67A: Sexually explicit material, including revenge pornography.

Section 67B: Sexual exploitation of children online.

Sections 72 and 72A: Confidentiality violations and improper use of personal information.

3. Indian Penal Code (IPC) and Bharatiya Nyaya Sanhita (BNS) :

Relevant IPC Sections:

Section 354A: Online sexual harassment.

Section 354C: Voyeurism (capturing or sharing private images).

Section 354D: Cyber stalking.

Section 509: Insulting the modesty of a woman.

Section 499–500: Online defamation.

Section 507: Anonymous criminal intimidation.

These provisions ensure that even when technology changes, the offence remains punishable.

4. Indecent Representation of Women (Prohibition) Act, 1986 :

This Act prohibits indecent representation of women through electronic media, advertisements, and publications. It complements the IT Act in cases of objectification and vulgar portrayal of women online.

Enforcement Agencies

1. Cyber Crime Cells:

These operate at state and district levels, investigating and handling cybercrimes.

2. National Coordination:

The Indian Cyber Crime Coordination Centre (I4C) enables interstate collaboration, and the National Cyber Crime Reporting Portal allows online complaints etc.

Role of judiciary

1. Online abuse harms dignity:

Bad messages, threats, or harassment online hurt a woman's respect and self-worth. Courts treat these acts as violations of dignity. They are not considered small or harmless mistakes.

2. Consent and privacy are important:

Court stress that no one can use or share a woman's photos, videos, or personal details without permission. Doing so is wrong and illegal. This helps victims get justice etc.

Preventive measures and suggestions for reducing cyber crime against women

1. Awareness and Digital Literacy :

Women should be educated about safe internet use. Knowing privacy settings, strong passwords, and online risks helps prevent cyber-crimes. Awareness programs in schools and colleges are very important.

2. Strong Cyber Laws and Strict Punishment :

Cyber laws should be properly enforced. Fast investigation and strict punishment for offenders create fear and reduce cyber-crimes against women.

3. Safe Use of Social Media :

Women should avoid sharing personal information, photos, phone numbers, or location on social media. Unknown friend requests and suspicious links should be avoided.

4. Reporting and Support Systems :

Victims should be encouraged to report cyber-crimes without fear or shame. Cyber cells, women helplines, and online complaint portals must be easily accessible.

5. Role of Family and Society :

Family members and society should support victims instead of blaming them. Moral support helps women report crimes confidently.

6. Role of Educational Institutions :

Schools and colleges should teach cyber safety and legal rights. Workshops and seminars can help students understand online risks.

Conclusion

Cyber-crime against women has become a serious challenge in the digital age, affecting their safety, privacy, and dignity. The increasing use of the internet and social media has created new opportunities for harassment, cyber stalking, identity theft, and online abuse. These crimes often cause psychological distress and discourage women from freely participating in digital spaces.

Although legal provisions exist to address cyber-crime, gaps in implementation, limited awareness, and delays in justice reduce their effectiveness. Therefore, stronger enforcement of cyber laws, faster legal procedures, and victim-friendly support mechanisms are essential.

Additionally, digital platforms must act responsibly by preventing misuse and ensuring user safety. A collective and sustained effort is necessary to ensure a safer and more inclusive online environment.

Reference :

- 1.Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence. *Violence Against Women*, 24(8), 1–24. (link unavailable).
- 2.Kumar, A. (2021). Cybercrime and women: Online harassment, stalking and blackmail – A sociological analysis. *International Journal of Current Research*. (link unavailable).
- 3.Patil, S. S. (2021). An empirical study on cyber-crimes against women in India. *International Journal of Legal Research*. (link unavailable).
- 4.Farhana, S. (2022). Cyber crimes and the victimization of women. *International Journal of Law, Management and Humanities*. (link unavailable).
- 5.Beevi, S. A., & Ramesh, K. (2023). Protecting women in the digital era: Legal challenges and safeguards. *National Journal of Cyber Security Law*.
- 5.Ahlawat, P., & Sharma, R. (2024). Cyber-crime against women: A socio-legal analysis. *ShodhKosh: Journal of Arts, Humanities and Social Sciences*.

