CYBERCRIME AND WOMEN: AN EMERGING CHALLENGE IN THE DIGITAL AGE

Dr. Varsha Sharma, Children Welfare Centre's College of Law

ABSTRACT

The digital revolution has opened up incredible opportunities for millions around the world, but it has also led to a troubling rise in cybercrimes, especially those aimed at women. In India and beyond, women are facing increasing risks from cyber threats like cyberstalking, trolling, online sexual harassment, revenge porn, and financial fraud. These offenses not only harm their personal dignity and mental well-being but also restrict their ability to engage safely in online spaces. Even though there are legal protections in place, many women remain vulnerable due to a lack of awareness, inadequate enforcement, and societal stigma. This article delves into the prevalence, nature, causes, and impacts of cybercrime against women, while also assessing how well current legal measures and support systems are working. Additionally, it offers a roadmap for prevention and redress, focusing on the importance of education, legal reforms, and enhancing digital safety.

Keywords: cybercrime, digital crime against women, online safety of women, gender based violence.

Introduction

The rapid rise of digital technologies in the 21st century has completely transformed how we interact, communicate, do business, and access information. The internet has become an essential tool for social inclusion, economic empowerment, and global connectivity. For women, especially, digital platforms have opened up incredible opportunities to share their voices, engage in public discussions, pursue education, and take part in economic and political activities. Yet, this same digital landscape that fosters women's empowerment also harbors risks, becoming a breeding ground for harassment, exploitation, and violence.

Cybercrime, which broadly refers to any illegal activity involving computers or networked devices, has morphed into a complex and borderless threat. When these crimes target women specifically, they take the form of online gender-based violence. This can include everything from cyberstalking and image-based sexual abuse (like revenge porn) to online harassment, trolling, financial fraud, identity theft, and defamation. What makes these offenses particularly dangerous is their anonymity, the ease with which they can spread, and the lasting harm they can cause through the repeated sharing of harmful content online.

The issue of cybercrime against women isn't limited to one region or country; it's a global problem. However, in India, the situation is exacerbated by deeply ingrained patriarchal values, low levels of digital literacy, and the social stigma that often silences women who dare to speak out against online abuse. Even with various legal protections under the Information Technology Act of 2000 and the Indian Penal Code (now replaced by Bharatiya Nyaya Sanhita (BNS) 2023), enforcement is weak, reporting is low, and awareness among women remains shockingly inadequate. The author has discussed provisions of Indian Penal Code in the present study.

Cybercrimes don't just threaten women's physical or financial safety—they also take a toll on their mental health, freedom of expression, reputation, and willingness to participate in public life. Experiencing online abuse can lead to anxiety, depression, and a host of other psychological challenges.

Research Objectives

1. To identify the most prevalent forms of cybercrime experienced by women in India.

2. To assess the psychological, emotional, and social consequences of cybercrime on women.

3. To understand the reasons for underreporting of cybercrimes by women.

4. To evaluate the effectiveness of existing legal mechanisms and law enforcement in dealing with such crimes.

5. To measure the level of awareness among women regarding cybercrime laws and digital safety practices.

6. To explore the role of social media platforms and tech companies in preventing online abuse.

7. To propose policy-level and grassroots-level recommendations to enhance digital safety for women.

Hypotheses

1. **H1:** Increased digital exposure correlates with higher vulnerability to cybercrimes among women.

2. **H2:** Lack of legal awareness among women contributes significantly to underreporting of cybercrimes.

3. **H3:** Women who experience cybercrime suffer more severe psychological effects compared to other forms of violence.

4. **H4:** The current legal and institutional framework is inadequate in addressing gendered cyber violence effectively.

5. **H5:** Targeted digital literacy and awareness programs can significantly reduce cybercrime incidents against women.

Types of Cybercrimes against Women

Cyberstalking

Cyberstalking is when someone repeatedly uses digital platforms to harass, intimidate, or keep

tabs on a victim, often with harmful intentions. It's more than just casual online interactions; it involves ongoing monitoring, unwanted messages, and surveillance through emails, messaging apps, social media, or even GPS devices. Women are especially at risk for cyberstalking, as offenders might track their movements, hack into personal accounts, or secretly observe their activities without permission. This invasion of privacy creates a constant atmosphere of fear and insecurity. In India, cyberstalking is addressed under Section 354D of the Indian Penal Code (IPC) and the Information Technology Act of 2000.

Online harassment covers a broad spectrum of abusive behaviors, including sending hurtful comments, sexist remarks, sexually explicit content, or even threats of violence through digital channels. Trolling is a specific type of targeted abuse where individuals deliberately provoke, insult, or humiliate women to silence their voices, particularly in public discussions. This is especially harmful to women activists, journalists, and professionals who face gender-based attacks simply for sharing their opinions online. Such harassment can lead to serious psychological distress, withdrawal from social media, and even concerns about physical safety. Sections 509 and 354A of the IPC address obscene comments and sexual harassment, while the Information Technology Act of 2000 criminalizes the sharing of offensive or threatening material.

Revenge Porn (Non-Consensual Pornography)

Revenge porn refers to the act of sharing or distributing private, intimate images or videos of a woman without her consent. This is often perpetrated by ex-partners as a form of revenge, blackmail, or coercion, and it fundamentally violates a woman's right to dignity and privacy. In our digital world, once such content is leaked, it can spread like wildfire, leading to devastating consequences for the victim's reputation and mental well-being. Many places, including India, recognize non-consensual pornography as a serious crime, with laws like Section 66E of the IT Act (which addresses privacy violations) and Sections 354C and 509 of the IPC (which deal with voyeurism and insulting a woman's modesty).

Morphing and Deepfakes

Morphing involves altering a woman's photos using editing software to create obscene, defamatory, or misleading images. With the rise of artificial intelligence, deepfakes have become a particularly alarming tool, allowing for the creation of highly realistic yet entirely

fake videos by overlaying faces or voices. This manipulated content can be weaponized for sexual exploitation, blackmail, political sabotage, or spreading false information. The fallout for victims can include damage to their reputation, career challenges, and significant mental distress. In India, these offenses are addressed under Sections 66C and 66E of the IT Act, as well as Sections 468 and 469 of the IPC (which cover forgery for cheating and defamation).

Doxxing

Doxxing is the deliberate act of revealing a woman's personal or sensitive information—like her home address, phone number, workplace details, or private conversations—on public platforms without her consent. This can lead to targeted harassment, physical stalking, or threats to the victim's safety. Doxxing represents a digital form of endangerment that blurs the lines between online abuse and real-world violence. In India, such actions can be prosecuted under Sections 503 and 507 of the IPC (which cover criminal intimidation and anonymous communication) and under the IT Act for privacy violations.

Phishing and Cyber Fraud

Phishing is all about those sneaky attempts to trick you into giving up your sensitive personal or financial information—think passwords, OTPs, or bank details—by pretending to be someone you trust, like a bank, an online store, or even a government service. Women, particularly those who might not be very tech-savvy, often find themselves as prime targets for these scams. They can get drawn in by fake job offers, dubious links, or emotional manipulation. The fallout can be serious, leading to financial losses, identity theft, or the misuse of personal information. In India, these kinds of crimes fall under Section 66C (identity theft) and Section 66D (cheating by impersonation using computer resources) of the IT Act, along with various IPC provisions related to cheating and fraud.

Impact of Cybercrime on Women

The impact of cybercrime on women is a pressing issue that has emerged as a modern form of violence, hitting women particularly hard and leaving scars that go well beyond the digital realm. While technology can empower, its misuse often leads to serious and lasting harm, especially in societies where patriarchal views and social stigma are prevalent. Women who fall victim to cyber harassment, stalking, or the non-consensual sharing of intimate images

often find themselves grappling with anxiety, depression, and post-traumatic stress disorder, especially when abusive content resurfaces online. The shame of public humiliation, coupled with the constant dread of being watched or judged, can chip away at self-esteem and push many women into emotional isolation.

On a societal level, cybercrime frequently results in victim-blaming, particularly in conservative communities where a woman's online presence is closely tied to her perceived morality. To escape harassment, many victims feel compelled to deactivate their accounts or limit their online interactions, which cuts them off from valuable professional, educational, and social opportunities. Manipulated images or slanderous content can damage personal relationships and permanently stain reputations, deepening the sense of isolation. In cultures where a woman's honor is linked to her digital behavior, such reputational harm can lead to life-altering consequences.

Female students and remote workers encounter harassment in virtual classrooms or meetings, making these digital spaces feel unsafe for learning and collaboration. This ongoing threat undermines digital confidence, hindering women from establishing their online presence, networking, or advancing in their careers in an increasingly interconnected world. Cybercrime also results in significant economic and privacy losses. Many women fall prey to phishing scams, investment fraud, and identity theft, with fraudsters impersonating them to commit crimes or extract money. Some victims lose employment opportunities when defamatory content spreads online. Infringements on privacy and dignity—such as the non-consensual distribution of intimate content, doxxing, and persistent cyberstalking through spyware or fake profiles—expose women to real-world dangers and create a lasting fear of surveillance. Collectively, these impacts make cybercrime against women a pressing social and legal concern, demanding stronger preventive measures, effective law enforcement, and robust victim support systems.

Recommendation

To tackle cybercrime against women effectively, India needs to adopt a comprehensive, gender-sensitive cybercrime law that recognizes the distinct nature and effects of online abuse on women. It's essential to set up dedicated cybercrime units staffed with trained female officers in every district, creating a safer and more welcoming environment for reporting incidents. The legal process should be streamlined with the introduction of cybercrime fast-track courts,

ensuring that investigations and trials happen swiftly, which can help alleviate the prolonged trauma that victims often face. Moreover, digital platforms should be held accountable with strict penalties if they fail to quickly remove reported abusive or non-consensual content

When it comes to prevention, awareness and education are key. Cyber safety and gender sensitivity should be woven into school and college curricula to promote respectful digital behavior from an early age. Nationwide digital literacy campaigns, especially aimed at women in rural and semi-urban areas, can empower them with the skills needed to recognize, prevent, and report cyber threats. Encouraging peer support networks and community policing initiatives can help cultivate a sense of shared responsibility, making both online and offline environments safer for women.

On the tech front, we should leverage technology to combat tech-enabled crimes. User-friendly apps that allow for anonymous reporting and immediate assistance can provide victims with a way to seek help without the fear of being exposed. AI-driven tools for the early detection of online threats, harmful content, and suspicious activities can facilitate quicker interventions. It’s vital for the government and tech companies to collaborate in creating safer algorithms and more robust content moderation systems that proactively shield women from harmful digital interactions.

Conclusion

Cybercrime against women has become a serious issue, transforming gender-based violence into a digital form. While the internet has improved communication and self-expression, it also enables harassment and control. Cybercrime harms women in many ways, affecting their mental health, safety, and professional growth. It's found in forms like cyberstalking, online abuse, identity theft, and financial fraud.

In India, these issues are intensified by low digital literacy, fear of victim-blaming, and ineffective legal responses. Cybercrime is dangerous due to its anonymity and viral impact, allowing offenders to harm victims without being physically present, leading to significant psychological distress. Although laws exist to combat cyber offenses, they often do not address women's needs adequately.

Improving the situation requires dedicated cybercrime units, fast-track courts, and victim

support systems. Education and preventive strategies are crucial for empowering women to protect themselves and participate online. Collaboration among social media companies, educational institutions, and civil society is necessary to create safer digital spaces. Protecting women from cybercrime is essential for dignity, equality, and justice. With legal reforms, social awareness, and community support, we can build a digital world where women feel safe and empowered.

REFERENCES

1. Sankhwar, S., Ahuja, R., Choubey, T., Jain, P., Jain, T., & Verma, M. (2023). Cybercrime in India: An analysis of crime against women in ever expanding digital space. Security and Privacy, 7 (1), e340. https://doi.org/10.1002/spy2.340

2. Tyagi, V. (2023). Victimization of women in cybercrime: An international perspective. International Journal of Law Management & Humanities, 6(6), 1888–1902. https://doi.org/10.1002/ijlmh.13701

3. Kaur, A. (2025). Cybercrime against women in India: Challenges and possible solutions. In *The techno-legal dynamics of cyber crimes in Industry 5.0 (Chap. 12). Wiley. https://doi.org/10.1002/9781394242177.ch12

4. Kasturi, Y., & Dar, M. A. (2024). Cybercrime in the digital age: Challenges and legal gaps in India's cybersecurity landscape. African Journal of Biomedical Research, 27 (6S), 212–224. https://doi.org/10.6313/ajbr.27.6S.212

5. Vaishnav, A., & Dewan, B. (2024). Cybercrime against women: Its evolution and effects on personal life. ShodhKosh: Journal of Visual and Performing Arts, 5 (1). [https://doi.org/10.5281/zenodo.1114457] (https://doi.org/10.5281/zenodo.1114457)

6. Dar, S. A., & Nagrath, D. (2022). Are women a soft target for cybercrime in India? Journal of Information Technology and Computing, 3(1), 23–31. https://doi.org/10.55529/jitc.31.23.31] (https://doi.org/10.55529/jitc.31.23.31)