WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Gendered nature of cybercrime: a study on the victimisation of women in online spaces

Shahla Azmi

Aligarh Muslim University

ABSTRACT :

Women are disproportionately the targets of cybercrime, a pressing issue that has escalated with the rapid advancement of digital technology. Based on a critical analysis of secondary data sources, such as official reports, scholarly studies, and existing literature, this study delves into the urgent need to address the gendered nature of cybercrime in India, particularly the victimisation of women. The most prevalent types of cybercrime against women, including revenge pornography, cyberstalking, and online harassment, are often underreported due to a lack of trust in law enforcement, societal stigma, and limited knowledge about available legal remedies. While legal frameworks exist, there are significant implementation and victim support gaps. To combat gendered cybercrime in India effectively, the study underscores the immediate necessity of victim-centred approaches, enhanced digital literacy, and stronger enforcement mechanisms. It's crucial for all of us, as academics, policymakers, and advocates, to play our part in addressing this issue.

Keywords: Cyber Risk, Cyber Security, Women, Victimisation, Social networking sites

Introduction

Cybercrime is a global phenomenon. The growth of technology has led to a rise in cybercrime and the victimization of women, significantly threatening individual security. Even though India is one of the few nations that passed the IT Act 2000 to tackle cybercrime, it does not address women's difficulties. The Information Technology Act of 2000 is a comprehensive legislation that deals with various aspects of cybercrime, including hacking, disseminating obscene content on the internet, and data tampering. However, this Act does not explicitly address the severe danger to women's security. Cyberbullying may harm anybody, including youngsters. Technical methods to secure computer systems are being introduced along with legislative measures to prevent and discourage illegal behaviour. However, this technology has no physical borders and may readily spread around the planet. As a result, criminals are increasingly found in locations other than those where their actions have an impact, and cyberspace is no exception. Cyberspace is a new frontier controlled by machines for information, and cybercrime refers to any illegal behaviour that uses a computer or network as a source, tool, or target. Cybercrime against women in India is a relatively recent phenomenon. When India began its journey into information technology, it prioritised safeguarding electronic commerce and communications under the Information Technology Act of 2000, leaving cyber socialising communications unaffected. The Act proved to be a half-baked statute since its scope included cyber-victimisation of women and cyber-laws in India. The current research is an effort to expose cybercrimes against women in India. Women's safety has long been a concern, particularly in India, where crimes against women are on the rise. Previously, it was restricted to highways or locations away from home. A lady used to feel comfortable at home, but that is no longer true. Home is becoming an equally unsafe environment. However, a restriction has been imposed on their computer displays. This is a serious worry. The rising prevalence of cybercrime against women has created uneasiness among women. They do not feel secure anymore. The consequences for them and society are even worse when we look at the big picture.

Cyberspace:

William Gibson, a science fiction writer, first used this phrase in 1984. In computer science, "cyberspace" is a worldwide network of computer networks facilitating data flow and exchange using the Transmission Control Protocol/Internet Protocol (TCP/IP). It is the virtual environment where human interaction occurs over computer networks, where users mentally travel through data matrices. In cyberspace, users chat, explore, research, and play on the Internet and other computer networks.

Evolution of Cyberviolence

Although gender-based violence has been around for a while, it has become much more pervasive and harmful since it has moved online. Women have been the targets of cyberstalking and harassment since the advent of email and chat rooms. With the emergence of social media, these threats have become more widespread, giving criminals tools to harass, exploit, and degrade others throughout the world.

Image-based abuse, which is occasionally referred to as "revenge porn," garnered significant attention in the 2010s. The lethal weapon against women was the non-consensual sharing of intimate photographs, which was often done as a form of vengeance or control. This form of abuse represented a shift in the mechanics of violence, as the internet's virality and permanence could potentially prolong the suffering of victims indefinitely.

Cyberviolence Against Women and Girls: The Forms

Online Harassment: This includes verbal harassment, trolling, and specific threats intended to silence or intimidate women.
"Image-Based Abuse (Revenge Porn): The sharing of private photographs without permission, usually to humiliate or control."
"Sextortion: Victims are coerced into offering personal photographs or favours under the threat of public exposure."
"Cyberstalking: Persistent observation or contact causes worry and anxiety."
"Deepfake Pornography: The use of artificial intelligence to create explicit material based on a person's image, usually for exploitation or blackmail."
"Gender-Based Hate Speech: The propagation of sexist or discriminatory information intended to degrade women."
Cyberflashing: Sending inappropriate photos via messaging applications or social media.

Types of Cyber Gender-Based Violence and Associated Statistics

Online gender-based violence (GBV) is a growing issue that affects millions of individuals worldwide, with children exposed to abuse more likely to experience or perpetrate it in their adult relationships. Digital domestic abuse is a particularly alarming form of online GBV, as it extends traditional domestic violence into online formats. It involves technology being used to harass, control, or manipulate a partner, such as unauthorised access to personal accounts, cyberflashing, coercing victims into sharing intimate content, and using social media to humiliate and degrade them.
The key distinction between traditional domestic abuse and digital domestic abuse lies in the medium through which the abusive behaviours are conducted. Technology advancements exacerbate digital domestic abuse by providing abusers with continuous access to their victims, making it harder for victims to find safety. Tools like GPS tracking, spyware, and social media monitoring allow abusers to surveil, harass, and control victims remotely with increasing ease. The anonymity of online spaces makes it easier for perpetrators to engage in cyberstalking, revenge porn, and other forms of digital abuse with reduced accountability. Victims often struggle to escape, as technology ensures that abuse can follow them wherever they go, blurring the lines between their public and private lives.
Cyberstalking is another category of online GBV involving persistent and threatening online behaviours. In 2023, 1 in 5 internet users felt at risk of online harassment or abuse. Every individual using the internet can face harmful interactions, with children and teenagers being especially vulnerable.
According to research, 20% of young women in the EU have experienced hypersexual harassment. In comparison, 58% of girls had encountered online harassment, with 50% reporting more online harassment than street harassment. A 2017 Amnesty International survey revealed that 36% of women in the UK felt that online harassment posed a threat to their physical safety. These findings underscore the growing prevalence and impact of online gender-based violence, emphasising the critical need for better legislative safeguards and digital security measures.

The NCRB Report on Cybercrime: Cybercrime in All Its Forms

Compared to the data from 2019, the number of cybercrime incidents in 2021 has increased by 18.4%, with a total of 52,974 cases registered under Cyber Crimes, a 5.9% increase from the 50,035 cases in 2020.
The percentage of the crime rate that falls under the category of total conducted offences increased from 3.7 in 2020 to 3.9 in 2021.
In 2021, fraud was responsible for most cybercrime instances (32,230 out of 52,974). This was followed by 4,555 occurrences of sexual exploitation (8.6% of the total) and extortion (5.4% of the reported events).
Nonetheless, Telangana recorded the most significant number of cybercrime occurrences in the country, with 2,691 instances in 2019 and over 10,300 in 2021, representing a 282% increase. The other top four states were Uttar Pradesh with almost 8,830 instances, Karnataka with over 8,100, Maharashtra with more than 5,560, and Assam with around 4,850 instances.

States report a drop in cybercrime

In 2021, cybercrime incidents decreased in eight of the 28 states compared to 2019.
Karnataka has seen a 32.3 per cent decrease in cybercrimes, while Uttar Pradesh has a 22.7 per cent decrease.

Offences under the IT Act 2000

The IT Act addresses offences including tampering with computer source documents, which include-
"Section 65 deals with the hacking of a computer system"
"Section 66 deals with the publishing of information that is obscene in electronic form"
"Section 67 deals with Access to the protected system"
"Section 70 deals with Breach of confidentiality and privacy"

The cause of the increase in cybercrime

Various reasons contribute to the growth in cybercrime.

- A rise in the amount of internet traffic.
- A lack of consciousness
- Both the police and the general population suffer from a lack of technical expertise.
- The challenges that arise while investigating cybercrimes

Why are cases not being registered?

Traditional and cyber investigations vary greatly; cybercrime investigation requires specific technological abilities. The police force lacks the instruments and training to conduct technological and cyber investigations.
The majority of crimes are unreported because women are fearful or ashamed, or because they do not know how to continue. Due to increased knowledge and comprehension, the tendency is currently shifting.

Difficulties in Combating Cybercrime Against Women

Even though cybercrimes against women are becoming more common, there are still insufficient legal remedies. Although it covers some aspects of cybercrime, the Information Technology Act of 2000 does not mention gender-based online offences. Jurisdictional enforcement is made more difficult by the transnational nature of cybercrimes. Furthermore, victim-blaming and social stigma frequently discourage women from reporting cybercrimes. Many victims are left without options as a result of the problem being made worse by low reporting rates and insufficient law enforcement responses.

Measures Taken by the Government

"Police" and "Public Order" are considered State subjects per the Seventh Schedule of the Indian Constitution.
The “Law Enforcement Agencies” (“LEAs”) of states and UTs are primarily responsible for the prevention, detection, investigation, and prosecution of offenses, including cybercrime. In prosecuting offenders, “LEAs” enforce the provisions of the law.
In contrast, the Central Government provides financial support and guidance to the State Governments to assist in developing their capacity through various programs.

India has been strengthening its framework for preventing cybercrime through some government measures.

Indian Cyber Crime Coordination Centre (I4C) under PMLA: The government has designated I4C as an authorised entity under the Prevention of Money Laundering Act (PMLA), allowing it to coordinate cyber-enabled financial crime investigations and share intelligence with agencies like the Enforcement Directorate (“ED”) and Financial Intelligence Unit (“FIU-IND”).
Citizens may use the National Cyber Crime Reporting Portal to report cyber frauds and financial scams, allowing authorities to take prompt action against cybercriminals.
Cyber Surakshit Bharat is a government project that aims to raise cybersecurity knowledge and resilience among companies and people.
Cyber Swachhta Kendra offers free tools for detecting and removing viruses from devices, assisting users in safeguarding their digital assets.
Cyber Command Centres: The Karnataka High Court has ordered the state government to build cyber command centres to combat rising cyber threats better.

Prevalence and Forms of Cybercrime Against Women

The National Crime Records Bureau (NCRB) reports that cybercrimes against women in India have significantly increased. The number of incidents involving the publication or transmission of sexually explicit content increased from 1,896 in 2021 to 2,251 in 2022. Other cybercrimes also observed significant increases, including creating false profiles, online harassment, and cyberstalking.
The COVID-19 experts noted a notable rise in cybercrime against women, particularly sextortion, during this time, which was exacerbated by the 19 lockdowns. Online complaints increased from 21 in February 2020 to 54 in April 2020, according to the National Commission for Women (“NCW”).

Initiatives and Recommendations

Many projects have been started to counteract the increase in cybercrimes directed against women. Under the Cyber Congress project in Telangana, public school students are taught to be "cyber ambassadors" to inform local populations on digital safety and cybercrime avoidance.
The National Commission for Women (NCW) also started the Digital Shakti program to raise digital awareness and enable women to negotiate online environments safely.
"Prevention is better than a cure". So, everyone who uses the internet should not share personal information with the public. This is especially important for women, who are more likely to become victims of theft.
It is imperative that social networking services, such as Facebook, maintain privacy restrictions regarding their information and photographs.
The more secure their private information and images are behind the screens, the less accessible they are.

Vishakha Singh, they should deliver a good lesson to every abuser and defamer. Despite sitting quietly and suffering, individuals should strive for justice because "if you do not fight against crime, crime will offend you".

Future Strategies for Addressing Cybercrime in India

Implement Advanced Cybersecurity Framework: The protection of critical information systems and networks can be achieved by investing in advanced cybersecurity technologies.
Cyber Hygiene Practices: It is imperative to implement effective cyber hygiene measures, including consistent software updates, secure online behaviour, and robust password administration.
Collaboration Strengthening: Develop partnerships with international organisations, law enforcement agencies, and other nations to facilitate the exchange of threat intelligence and best practices, as well as to coordinate efforts to investigate and prosecute cross-border cybercrimes.
Public Awareness and Education: Conduct comprehensive awareness campaigns to educate the public on the importance of cybersecurity, secure online practices, and prevalent cyber hazards.
Promote the Use of Cyber Insurance: To mitigate the financial losses that result from cyber events and incidents.
Furthermore, cyber-risk coverage is instrumental in paying legal fees, investigators, crisis communicators, and customer credits or reimbursements, all associated with remediation.

The CCPWC program aims to prevent cybercrime against women and children.

Under the "Cyber Crime Prevention against Women & Children (CCPWC)" program, the Ministry of Home Affairs has given all States and UTs financial support to improve their cybercrime response mechanisms.
The program aims to assist the states in employing junior cyber consultants, training, and establishing cyber forensic-cum-training labs. In 28 States, cyber forensic and training labs have been set up as part of the program.

Raising awareness of cybercrimes

The Central Government has implemented several measures to enhance public awareness of cybercrimes, such as the publication of warnings and advisories, the development of cyber forensic technology, and the provision of capacity building and training for law enforcement, prosecutors, and judicial officials.
The Ministry of Electronics and Information Technology ("MeitY") conducts programs to increase public awareness of information security. Books, films, and internet resources devoted to information security are produced for children, parents, and other users.

Cyber Crime Coordination Centre (I4C)

The government established "the Indian Cyber Crime Coordination Centre (I4C)" to provide a framework and ecosystem for LEAs to address cybercrimes comprehensively.
In order to resolve the issue of jurisdictional complexity, the I4C has established "Joint Cyber Coordination Teams" in Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati, which are defined by hotspots/areas for cybercrime.
These teams are responsible for establishing a practical coordinating framework for the LEAs.

Portal for Reporting Cybercrimes Nationwide

The government created the National Cyber Crime Reporting Portal to allow the public to report various cybercrimes, with an emphasis on cybercrimes against women and children (www.cybercrime.gov.in).
Additionally, a Citizen Financial Cyber Fraud Reporting and Management System module has been included to facilitate quicker reporting of financial fraud and deter criminal activity.

Conclusion

The primary objective of cyber socialising is to enable users to connect with both old and new acquaintances, expand their networks, and engage in social activities without physically attending social events. Nevertheless, this is not a zone that is entirely free of hazards. The primary disadvantage of cyber-socialising is the ambiguous reliability of the "virtual friend" we encounter daily in the "Social Networking Websites" ("SNWs)". Simultaneously, numerous users regard cyber socializing as an environment that violates their freedom of speech and expression (Citron, 2005). This attracts a variety of offences, including cyberbullying, cyberplace, cyberhate speech, and cyber genital taunting. Online socialising is never entirely risk-free for women, primarily because of their sexual orientation. The SNWs are the location where most cybercrimes targeting women occur (Citron, 2009; Halder & Jaishankar, 2008). However, online societies are no exception to the rule that no society can be crime-free. The prevalence of cybercrime is increasing (Wall, 2007) due to the proliferation of SNWs, emails, and online chat forums.
Social networking websites enable various social activities to be carried out in cyberspace. Online socialising is equally fragile as in-person socialising. However, the patterns may alter because of the high-tech nature of the offences. The assailants may or may not be known to the victims, and the reasons and motivations for victimisation are often emotional. The harasser exploits the larger internet platform to victimise the target using fictitious identities.

Furthermore, unequipped, ill-fitting, or emerging laws in which such acts are not identified or have yet to be recognised contribute to the daily expansion of the pattern of victimisation.

The two primary factors contributing to the rise in online victimisation of women in the SNWs are a lack of appropriate gender-sensitive universal cyber legislation and a lack of understanding of safety measures among SNWs users. The SNWs are seen as a big worldwide platform on which to communicate one's views, thoughts, and sentiments toward others. Each participant is expected to utilise this platform at risk (Wall, 2007). Unfortunately, there are fewer rules and policy guidelines to control the internet, which allows offenders unlimited freedom. This is an excellent illustration of how a lack of understanding of cyber-social standards and norms and lax legislation may lead to criminalisation in online socialisation. Laws may provide a clear boundary for regulating an individual's behaviour. However, it is up to the person to apply the rules to make their living place safer and more attractive, including the internet.

REFERENCES

- Graham, N. (2018). Cyber crimes against women in India. *Asian Journal of Women's Studies*, *24*(3), 413–417. https://doi.org/10.1080/12259276.2018.1496783
- Jain, M. (2017). Victimization of women beneath cyberspace in Indian upbringing. Bharati Law Review, 1(1), 1-11.
- Halder, D., & Karuppannan, J. (2009). Cyber socializing and victimization of women. The Journal on Victimization, 12(3), 5-26.
- Yadav, H. (2022). UNVEILING THE DARK SIDE OF CYBERSPACE : A STUDY OF CYBER CRIMES AGAINST WOMEN IN INDIA Keywords : Cyber Risk , Cyber Security , Women. 11, 3408–3421.
- Center, H. R. R. (2025b, April 7). The digital age and the escalation of cyber Gender-Based violence. HRRC. https://www.humanrightsresearch.org/post/the-digital-age-and-the-escalation-of-cyber-gender-based-violence
- Raj, P. (2024, December 17). Cybercrime against women - ClearIAS. ClearIAS. https://www.clearias.com/cybercrime-against-women/
- PWOnlyIAS. (2024b, April 17). NCRB data on cyber crime in India - PWOnlyIAS. PWOnlyIAS. https://pwonlyias.com/editorial-analysis/growing-cyber-crime-in-india/
- http://delhicourts.nic.in/ejournals/CYBER%20LAW.pd.
- Major boost to India's fight against Cyber-Enabled money laundering: I4C gains PMLA Authority. (n.d.). https://www.lawweb.in/2025/04/major-boost-to-indias-fight-against.html
- Plumber, M., & Law, L. (2025, April 28). Live law. Live Law. https://www.livelaw.in/high-court/karnataka-high-court/karnataka-high-court-order-cyber-command-centres-karnataka-government-290613
- Vishaka and Ors v. State of Rajasthan and Ors.(JT 1997 (7) SC
- https://www.wionews.com/india-news/significant-increase-in-cybercrime-against-women-during-coronavirus-lockdown-in-india-296071
- https://www.researchgate.net/publication/385122103_CYBER_CRIMES_AGAINST_WOMEN_IN_INDIA