International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Navigating Cybercrime: The Impact on Women in India and the Need for Digital Safety

Vibha Saraswati

Assistant Professor, Department of Geography, Rajiv Gandhi Government College, Chaura Maidan, Shimla 171004, India
Email: *saraswativibhacollege[at]gmail.com*

Abstract: ***The digital era has brought unprecedented changes in the society, opening new avenues for communication, business and education. The internet can be viewed as a double-edged sword on one hand it has made the world a global village and on the other hand it has given birth to various maladies that make the user vulnerable to various malicious activities, where the offender is concealed. Use of social media platforms have introduced various forms of cybercrime, with women being disproportionately affected. Being a victim of cybercrime could be the most traumatic experience for women especially in a country like India where society looks down upon women if their name is involved in matters which question their integrity. Women often shy away from reporting any instances of cybercrime because they fear defamation. Cybercrime affects women the most by subjecting them to mental and emotional stress, humiliation and depression. In India cybercrimes against women have escalated significantly, presenting unique challenges that require comprehensive strategies for mitigation and control. Proper digital awareness can help inculcate safe online working environment for women. In such a scenario the role of Government and NGOs to educate women about their rights and importance of reporting cyberattacks become significant. The Indian Penal Code includes sections which addresses cases related to sexual harassment against women. The Information Technology Act also has sections which addresses the same offences. Access to internet is fast becoming a necessity for the economic well-being and is increasingly viewed as a fundamental human right therefore, it becomes important to ensure that this digital space is safe and an empowering place for all especially women and girls.***

Keywords: cybercrime, cyberstalking, phishing, digital literacy, online safety tools

1. Introduction

The advancement in Internet has made the old way of communication obsolete. The information we acquire using the internet is made available to us with the blink of an eye. It must not be forgotten that with the fast-growing digital technology on one hand and absence of digital literacy on the other, the user can also become vulnerable to cyberattacks. The internet has changed the world for the better in many ways however, the incidents of cyberattacks have also risen in tandem with the expansion of the internet (James Dobbins *et al.*, 2015). Cybercrime happens when a computer is used to carry out illegal activities. Cybercrime against women encompasses a wide range of malicious activities conducted via the internet or electronic devices. "Online violence could occur in all spheres but perhaps falls most readily under community violence including sexual harassment, threats and intimidation at work, in educational institutions and elsewhere. Example of harm related to online sexual violence can be physical or psychological. Online physical harm means using social media to gain trust or arrange to meet in physical space and commit sexual assault, posting personal /locational information and encouraging others to perpetrate sexual assault recording or distributing images of sexual assault. Psychological online harm includes sexual threats, sending repeated and unwanted sexual communication, using social networking sites to promote sexual violence or vilify survivors of sexual assault or non-consensual sharing of sexually explicit images." (Jordan Fairbairn, 2015). For, women in India, the most common forms of cybercrimes include cyberstalking, harassment, revenge porn, phishing, financial scams, impersonation and fake profiles (Dutta, 2023). Finding information about cyberattacks is a challenge for the corporate and government entities. The governments can curb crime by creating strict norms. If the lawbreaker is arrested, convicted and sentenced he will dissuade from doing such crimes again and again (Brenner, Susan. W, 2012). This paper explores the nature of cybercrime against women in India, examines the legal framework, highlights the challenges faced, and proposes suggestions to enhance online safety for women.

Major Cybercrimes against Women:

There are a lot of risks associated with cybercrime. Cybercriminals breach financial security as well as personal information of the victim. Therefore, it becomes pertinent to know about the prevalent cybercrimes.

Cyberstalking and Harassment

Women in India frequently face cyberstalking through social media, emails, and messaging platforms. The act of communicating words or images using electronic devices directed at a someone causing anguish and serving no legitimate purpose is punishable by law. (Brenner, Susan. W, 2012). Harassment includes threatening messages, obscene content, or unsolicited sexual advances, creating a hostile online environment.

Cyberpornography and Non-Consensual Image Sharing

Cyberpornography means using internet to show sexual acts in order to cause sexual excitement. In the domain of cyberspace, where popular understanding of women's bodies become dominated by sexually explicit or compromising images makes the cybersex industry grows (Anna Sampaio; Janni Aragon,2001). Women in particular are more vulnerable to such cybercrimes. Another crime under this head is Revenge porn that involves the distribution of private, intimate images or videos without the individual's consent, typically by an ex-partner seeking revenge. This form of cybercrime leads to significant emotional trauma, social stigma, and in some cases, severe reputational damage. Non-consensual image sharing can also occur when hackers gain

unauthorized access to a woman's digital devices or social media accounts.

Phishing and Spoofing

The Anti-Phishing Working Group defines phishing as "a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers personal, identity and financial account credentials." (J. Anthony Vittal,2005). Women are easy targets of Phishing, just by clicking the link the cybercriminals get money transferred into their accounts leading to identity theft and financial loss. Cybercriminals often exploit the trust and emotional vulnerability of women to execute these scams. In Spoofing the hacker tries to acquire the identity of the genuine user while in Phishing the hacker reveals some sensitive data to the user in order to exploit him

Fake Profiles and Morphing

The sophistication of new technologies enables morphing and construction of fake images or videos which are often perceived to be "real" or "authentic" (Anita Gurumurthy; Niveditha Menon,2009). Impersonations can cause significant reputational damage and distress to the victims. Morphing is the unauthorized act of editing the original photograph of a person with the intent of misusing it. Photographs of women are downloaded from websites, morphed and then reposted on different websites creating fake profiles.

Cyber Defamation

This the act of ridiculing another person, groups or organizations by a post on the internet. It also includes the use of abusive language on cyberspace. Publishing false statement about an individual with the intention of demeaning his reputation. Cyber Defamation is seen both as a civil and a criminal offence (Kukreja,2022). Women face rejection from society if their fake images go viral on any social platform.

Cyberbullying

Cyberbullying is the use of digital technology to knowingly annoy someone. It can also be called harassment using the social media. Here the bully remains unknown (Evelena Landstedt; Susanne Persson (2014). The term 'Cyberbullying was first coined by 'Bill Belsay' a Canadian educator. He defines it as "using both information technology and communication technology beyond a limit to humiliate a person and harm his reputation.

Alarming figures on Cybercrime against Women in India

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crime in its publication 'Crime in India'. The report says prevalence of cybercrime against women in India has been rising steadily. According to NCRB cybercrime cases targeting women have shown a significant increase over the years. For instance, in 2019, there were 8,378 reported cases of cybercrime, with a notable percentage involving offenses against women.60.4% of cybercrime cases were for fraud and sexual exploitation. Crime against women in India was up by 4% in 2023 this involved cruelty of husband and his relatives, abduction assaults and rapes (Jha, 2024). The cases escalating from 3,71,503 in 2020 to 4,45,256 in 2022 compared to 2021's 4,28,278 cases, the 2022 figures marked a concerning increase. A study conducted by the Future Crime Research Foundation and IIT Kanpur discloses that there are 35 cybercrime hotspots in India out of which the top 10 together account for 80% of cybercrime related cases in India (Neeraj Soni, March 2024).

Evidences of Cybercrime

Examining specific case studies can provide a deeper understanding of the impact of cybercrime on women in India and highlight successful interventions.

Case Study 1: Cyberstalking

In 2003 the first cyber stalking complaint in India was lodged by Ritu Kohli. Her husband's friend posted her name and contact details on a chatting site without her permission, a complaint was filed by the sufferer. The preparator was sentenced under Section 509 of IPC which entails three years of imprisonment coupled with fine. The case was decided in the favour of the victim Rohitlohia, 2022).

Case Study 2: Revenge Porn

Examples of harm related to online social violence can be physical as well as psychological (Jordan Fairbairn, 2015). Case Law: State of west Bengal VS Animeshi Boxi, 2017. In this case the victim had a relationship with the offender who shared some intimate pictures of her on porn sites with details of her and her family and later blackmailed her to be with him. The court decided in favour of the victim. The criminal was sentenced under Section 354A,354C, 354 and 509 of IPC as well as Section 66E, 66C and 67A of IT act (India Law Office, 2023).

Why is Cybercrime in India on the rise?

India is ranked at 10th in Global Cybersecurity Index 2020 by International Telecommunication Union (ITU) (Ghafoor, 2023). The increase in the number of cybercrime cases can be attributed to the following causes:

Underreporting:

Many women do not report cybercrimes due to fear of social stigma, lack of awareness about legal remedies, and mistrust in the legal system. Underreporting perpetuates the cycle of abuse and allows offenders to evade justice. The number of cybercrime cases are showing a troubling increase in number and one is prone to think that government agencies are engaged in new ways to curb it but the truth remains that most cyberattacks go unreported.

Lack of Digital Literacy:

"Inequality Report 2022: Digital Divide" by Oxfam says that only 38% of the households in India are digitally literate moreover, only 31% of the rural population uses the internet as compared to 67% of the urban population. A significant portion of the population, particularly in rural areas, lacks basic digital literacy (Indian Development Review, 2023). This makes women more vulnerable to cybercrimes as they may not recognize phishing attempts or know how to protect their online privacy.

Insufficient Legislation:

The country where the preparator is based may have a legislation which is incompatible with that of the victim's country. This makes investigation procedures inconvenient (Jeffray & Feakin, 2015). In many cases the reluctance of the police to register First Information Report (FIR) especially

those of sensitive nature, is not an unfamiliar phenomenon (NCRB, 2008). Law enforcement agencies often lack specialized training to handle cybercrime cases effectively. This can lead to inadequate investigations and failure to bring offenders to justice.

How India is combatting the problem?

India has been working on enhancing her capabilities to handle cybercrime. Cyber and Information Security (C&IS) Division deals with matters relating to cybersecurity, cybercrime, National Information Security Policy and Guidelines (NISPG) and implementation of NISPG (Ministry of Home Affairs https://www.mha.gov.in).The legal framework and other support system shall make its citizens less vulnerable to incidences of cybercrime.

Law protecting Women in Cyberspace

India has developed a robust legal framework to address cybercrime, particularly offenses targeting women. Key legislation includes the Information Technology Act, 2000, and relevant sections of the Indian Penal Code (IPC).

Information Technology Act, 2000

The Act permits filing of documents in electronic form. It lists certain cyber offences allowing the law enforcement agencies to prevent cybercrimes (Devashish Bharuka, 2022). Specific sections relevant to crimes against women include:

Section 66E: Pertains to the violation of privacy by capturing, publishing, or transmitting images of a private area of any person without their consent. Violations can result in imprisonment and fines.

Section 67: Addresses the publication or transmission of obscene material in electronic form. Offenders can face imprisonment and fines.

Section 67A: Relates to the publication or transmission of sexually explicit material. This section carries stricter penalties, including longer imprisonment terms and higher fines.

Indian Penal Code (IPC)

The IPC also includes provisions that can be applied to cybercrimes against women. The important ones are highlighted as under:

Section 354D: Specifically addresses stalking, including cyberstalking, and prescribes imprisonment and fines for offenders.

Section 499: Covers defamation, which can be applied to cases involving the creation of fake profiles or the distribution of defamatory content.

Section 507: Deals with criminal intimidation by anonymous communication, applicable in cases of threatening messages or emails.

Support System to tackle cybercrime

A robust support system is needed to keep people safe in an online environment. Awareness of such systems will ensure lesser online abuse and exploitation. A familiarity with the below mentioned has been suggested for the online users.

Cyber Police Stations, Portals and Helplines

Several states in India have established dedicated cyber police stations to handle cybercrime cases efficiently. National Cyber Crime Reporting Portal has been launched as a part of 14C to enable complaints of cybercrime with special focus on cybercrime against women and children. A tollfree Helpline number '1930' has been made functional to get assistance in lodging online cyber complaints. Additionally, the Ministry of Home Affairs has also launched the Cyber Crime Helpline 155260, providing a platform for victims to report incidents and seek assistance.

NGOs and Support Schemes

Cyber Peace Foundation: This organization works towards creating a secure and peaceful cyberspace. It offers resources and support to victims of cybercrime and conducts awareness programs.

National Commission for Women (NCW): The NCW addresses issues related to women's rights and provides a platform for women to report cybercrimes. It also works with law enforcement to ensure timely action.

Cyber Crime Prevention against Women and Children (CCPWC) scheme:

Ministry of Home Affairs has provided financial assistance to all the States and Union Territories. Under this initiative cyber forensic-cum-training laboratories have been set up in all states across the country.

Online Safety Tools

Encouraging the use of online safety tools can help women protect their digital privacy. Key tools include:

- Privacy Settings: Using privacy settings on social media platforms to control who can view and interact with their profiles.
- Two-Factor Authentication (2FA): Implementing 2FA for online accounts to add an extra layer of security.
- Anti-Virus Software: Installing and regularly updating anti-virus software to protect against malware and phishing attacks.

2. Conclusion

Cybercrime against women can lead to mental and emotional stress causing humiliation and depression. It is a multifaceted issue that requires a concerted effort from all sectors of society. While significant strides have been made in terms of legal frameworks and institutional mechanisms, much more needs to be done to address the underlying societal and cultural factors that perpetuate these crimes. Law makers should strive towards ensuring that use of technology advances in a healthy way by fostering a culture of awareness, support, and empowerment. Providing specialized training for police officers and judicial personnel on handling cybercrime cases with a focus on gender sensitive approach. Partnering with technology companies to promote safer online practices and provide resources for reporting and preventing crime. India can create a safer digital environment for women,

ensuring their right to participate in the online world free from fear and harassment.

References

[1] Gurumurthy, A., N. Menon. (2009). Violence against Women in Cyberspace. *Economic and Political Weekly*. Vol. 44, No. 40.
[2] Sampaio, A., J. Aragon. (2001). Filtered Feminism: Cybersex, E-commerce and the Construction of Women's Bodies in Cyberspace. *Women's Studies Quarterly*, Vol.29, No. 3/4.
[3] Vittal., A. J.. (2005). Phishing, Pharming and other Scams. *G.P Solo*, Vol.22, No.8, Privacy and Security, (2005).
[4] Brenner, Susan W. (2012). Cybercrime and Law Challenges; Issues and Outcomes. Northeastern University Press, Boston.
[5] Jeffray, C. & T. Feakin., (2015). "Underground Web: The Cybercrime Challenge", (2015). Australian Strategic Policy Institute, Special Report. https://www.aspi.org.au/report/underground-web-cybercrime-challenge.
[6] Bharuka. D. (2022). Indian Information Technology Act, 2000 Criminal Prosecution Made Easy for Cyber Psychos. *Journal of Indian Law Institute*, Vol. 44, No.3.
[7] Dutta. L. (2023). A Study on Cybercrime against Women: Special reference to Dibrugarh University. *International Journal of Innovative Science and Research Technology.* Vol. 8. No. 8.
[8] Landstedt. E. and S. Persson. (2014). Bullying, Cyberbullying and Mental Health in Young People", *Scandinavian Journal of Public Health*, Vol.42, No.4.
[9] Ghafoor. W. (2003). Enhancing Cyber Resilience: Challenges and Opportunities in South Asia. Institute of Regional Studies. Vol.41, No.8 (1).
[10] National Cybercrime Report Portal: https://cybercrime.gov.in/
[11] Dobbins, J., R.H. Solomon, M.S. Chase, R.Henry, F.S.Larrabbe, R.J. Lempert, A.M. Lieman, J. Marlini, D. Ochmanek & H.J.Shalz. (2015). Choices for America in a Turbulent World, Strategic Rethink, RAND Corporation.
[12] Jha. R. (2024). Crime in India: A Critical Review of Data Collection and Analysis. *Policy Commons*, Observer Research Foundation, Issue No. 710.
[13] Fairbairn, J. (2015). Rape Threats and Revenge Porn: Defining Sexual Violence in the Digital Age. In J. Bailey & V. Steeves (Eds.), eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices (pp. 229–252). University of Ottawa Press. http://www.jstor.org/stable/j.ctt15nmj7f.13
[14] Bailey, J., & Steeves, V. (Eds.). (2015). eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices. University of Ottawa Press. http://www.jstor.org/stable/j.ctt15nmj7f
[15] Kukreja, D. (2022). Defamation and Virtual World: Issues and Challenges. *Law Essentials Journal*. Vol.3 No.46.
[16] India Development Review (2023). The digital divide in India: From bad to worse. Available online at: https://idronline.org/article/inequality/indias-digital-divide-from-bad-to-worse/
[17] National Crime Record Bureau Reports: Various Years.
[18] Soni, N. (2024). Emerging Cyber Crime Hotspots. *Cyberspace*, available online at www.cybre.org/resources/blog/emergingcybercrime hotspots.
[19] Lohia, R. (2022). Cyberstalking in India", Legal Service India e-Journal.