Page 1388 - 1394 **DOI:** *https://doij.org/10.10000/IJLMH.119843*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Cyber Crimes against Women in India

NAVANEETHAKRISHNAN. T[1] AND MANOHARAN C[2]

ABSTRACT

In our nation, women are accorded a unique status. They are revered as deities. However, as society has become more modern, their fundamental rights have been infringed. India's information technology industry is expanding quickly. Cybercrime is on the rise in tandem with the widespread use of computers. Furthermore, the majority of cybercrime victims in our nation are women. Cybercrime comes in many forms, such as cyberstalking, cyberdefamation, and cybermorphing. Emails are being used to harass women. They deal with the issue of cyberbullying, which is prevalent these days. To prevent these kinds of crimes, we have the Information Technology Act of 2000. With an emphasis on the legal system and enforcement strategies, this research critically investigates the scope and character of cybercrimes against women in India. Online harassment, cyberstalking, and revenge pornography are the most prevalent cybercrimes, according to the survey, and they frequently go undetected because people are unaware of them and don't trust the police. India's present legal system is insufficient to combat cybercrimes against women, and law enforcement organizations require stronger resources and training, as well as more women's education about the hazards and legal rights.

Keywords: *Cyber Risk,Cyber crime,Cyber stalking, Cyber defamation*

I. INTRODUCTION

The term "cybercrime" describes unlawful actions committed via the use of the internet or other digital devices. Financial fraud, cyberbullying, hacking, and online harassment are just a few of the many acts that fall under the umbrella of cybercrime. Unfortunately, in India, where cybercrimes against women have quickly escalated in recent years, women have been disproportionately harmed by cybercrime.

In India, cybercrime has a serious negative impact on women's mental and physical health. As social media and internet platforms have grown in popularity, cyberbullying and online harassment which specifically targets women have become common place in India[3].In India, there are several forms of cybercrimes against women, such as online stalking, cyberbullying, and online harassment. Given that India is one of the top five nations in the world for

[1] Author is a Guest Lecturer at Government Law College, Coimbatore, India.
[2] Author is an Advocate at Judicial Magistrate and Munsiff court, Alangulam, India.
[3] National Crime Records Bureau. (2020). Crime in India. Retrieved from https://ncrb.gov.in/en/crime-india

 [ISSN 2581-5369]

cybercrime, the country's present cybersecurity situation is concerning. There are still a lot of holes in India's cybersecurity implementation, even with the government's attempts to make cybersecurity laws and regulations stronger. The issue is also made worse by the general public's and law enforcement agencies' ignorance of cybersecurity.[4] The government, law enforcement, and civil society organizations must respond quickly to the various forms of cybercrimes. A complete strategy is required to combat cybercrime, one that includes boosting public awareness, fortifying cybersecurity laws and regulations, and offering assistance to victims.

Meaning of Cybercrime

There is no mention of cybercrime in the Information Technology Act of 2000 or any other Indian law. The word "cybercrime" refers to crimes committed online when the offender is anonymous and just has to utilize a computer screen to avoid making eye contact with the victim. In a cybercrime, the computer or data is either the intended victim, the intended result of the crime, or a tool that provides the necessary inputs to enable the conduct of another crime.

II. THE ROLE OF WOMEN IN CYBERCRIMES[5]

During the epidemic, women and children were the most vulnerable members of society, making them easy targets for cybercriminals, while adults and males fell prey to a number of cybercrime schemes. During the epidemic, women—especially housewives and social media users—were vulnerable to these crimes. Cybercrime attacks against women surged during a lockdown, It forced people to utilize the internet for work, play, education, and social reasons. Working women began working from home with the advent of computers, cellphones, and the internet. For online courses and other academic endeavors, women who are still enrolled in school are forced to utilize the internet. Since most women were utilizing social media sites and one or more online platforms for educational, professional, and recreational objectives, the rate of cybercrime against women began to rise during this period. Because the entire nation was under lockdown, criminals were unable to physically damage the victim, so they began torturing them mentally and emotionally.

[4] Sharma, R. (2018). Cyber Crimes Against Women in India: An Analysis. Journal of Information Technology and Economic Development, 9(2), 18-33. https://www.jited.org/index.php/jited/article/view/128/79

[5] *Cyber Crimes Against Women: Legal Service India - law articles - legal resources* (no date) *Legal Service India - Law, Lawyers and Legal Resources*. Available at: https://www.legalserviceindia.com/legal/article-8918-cyber-crimes-against-women.html (Accessed: 21 May 2025).

III. DIFFERENT TYPES OF CYBERCRIMES AFFECTING WOMEN[6]

Among the many cybercrimes that are perpetrated against people and society as a whole, the following crimes target women in particular:

- **Sextortion**

Sextortion was the most prevalent cybercrime committed against women throughout the pandemic. The criminals began extorting money or sexual favors from their victims by whitemailing them with their private photos or photoshopped images. The criminals intimidated women and demanded letters or sexual video conferences from them to vent their frustration over the outbreak. In order to obtain money from the victims, they also felt empowered to threaten them with their manipulated photographs because they were impoverished.

- **Phishing**

Criminals use phony emails that contain links to specific websites in an attempt to trick victims into divulging personal information, such as passwords and contact details, or to infect their devices with harmful viruses as soon as the link is clicked in order to profit during the lockdown. It looks like these emails and texts are real. The attackers then use the victim's bank account and other confidential information to conduct dubious transactions from the victim's bank account to their own.

- **Pornography**

Offenders engaged in online sexual assaults on women during the pandemic, modifying the victim's photograph and putting it in pornographic content.

- **Stalking**

Among other things, it involved contacting the victim or making an effort to interact with her on social media or over the phone despite her blatant lack of interest, leaving threatening notes on her page, and continuously calling her by phone and email.

- **Hacking**

Online news reading became popular throughout the pandemic. Now more than ever, there are instances of misinformation and fake news. Cyber hackers targeted the women after they clicked on fraudulent URLs. The spyware activated the microphone and camera on their

[6] *Cyber Crimes Against Women: Legal Service India - law articles - legal resources* (no date) *Legal Service India - Law, Lawyers and Legal Resources*. Available at: https://www.legalserviceindia.com/legal/article-8918-cyber-crimes-against-women.html (Accessed: 21 May 2025).

phones, downloaded all of their personal data, and captured their private images and videos. Criminals then utilize these images and bits of information to commit crimes like extortion.

- **Cyber-bullying**

This involves threatening the victim with rape or murder, posting derogatory, abusive, and inaccurate information about them on social media, and requesting payment to have it taken down. It also include making offensive remarks on the victim's posts. Examples of digital or communication technology that are used for bullying and harassment include computers, laptops, and cell phones.

- **Cybersex trafficking**

The victim does not interact physically with the offender, which sets it apart from physical sex trafficking. The practice of a dealer broadcasting, recording, or photographing the victim having sex or personal activities from a central place and then selling the footage online to customers and sexual predators is known as cybersex trafficking. The perpetrators have coerced, coerced, and threatened women into engaging in cybersex trafficking, which is a kind of sexual abuse of women.

IV. LEGAL PROVISIONS REGARDING CYBERCRIME AGAINST WOMEN

A. Bharatiya Nyaya Sanhita (BNS), 2023[7]

- **Section 294** [8]

It specializes in the dissemination of pornographic content, even through technological means. In addition to fines and incarceration, repeat offenders face greater punishments.

- **Section 77**

It emphasizes taking or disseminating images of a woman's intimate areas or behaviors without her permission, which is known as "voyeurism."

- **Section 303**

Particularly, theft involving data, cell phones, or computer hardware and software is covered in this area. It provides a legal foundation for the prosecution of those involved in cyber theft. However, when specific legislation like the IT Act are invoked, their application takes precedence.

[7] Bharatiya Nyaya Sanhita (BNS), 2023

[8] Magon, Adv.D. (2024a) *Cyber crime punishments under BNS (Bharatiya Nyaya Sanhita)*, *JudiX*. Available at: https://www.myjudix.com/post/cybercrime-punishments-under-bns-bharatiya-nyaya-sanhita (Accessed: 21 May 2025).

- **Section 78**

It describes the crime of stalking, both online and offline. imposes jail time and fines for using physical or technological methods to harass or observe a woman.

- **Section 317**

It pertains to situations in which someone obtains stolen computers, data, or cell phones. Even third-party possession of such property carries consequences.

- **Section 318**

It Deals with scams, such as cyber frauds, building fake websites, and password theft. imposes different jail terms and penalties according on the seriousness of the infraction.

- **Section 336**

It addresses crimes such as online forgery and email spoofing. imposes fines, jail time, or both. This part also applies when someone's reputation is being harmed by forgery.

- **Section 356**

It punishes defamation, including sending emails containing offensive material. imposes penalties and incarceration

B. Information Technology Act 2000[9]

The Information Technology Act of 2001 is a vital tool in the fight against cybercrime. Although some of the legislation's provisions concern crimes against human bodies, the statute primarily deals with internet transactions. The Act's principal provisions are as follows:

- **Section 67**

The IT Act's Section 67 forbids the publication and dissemination of pornographic material online that compromises morals and public order.

It is predicated on IPC Sec. 292. However, the IT Act of 2000 imposes harsher penalties. This offense is subject to bail.

- **Section 66C**

Identity theft is a crime covered by Section 66 C. The aforementioned offense is bailable, meaning that the accused has the right to bail even if they are arrested.

[9] The Information Technology Act, 2000 (IT Act)

 [ISSN 2581-5369]

- **Section 66D**

Section 66 D declares that an individual has committed the crime of cheating if he uses a computer system, computer networks, computer resources, or communication devices to pose as someone who has already psassed away.

- **Section 66E**

Section 66E has been strengthened to include the crime of privacy breach. The following actions that are required must be taken: Photographing, Publishing, and transforming

V. PREVENTING CYBER CRIMES AGAINST WOMEN[10]

India is seeing an increase in cybercrimes targeting women, hence it is imperative that women take precautions to avoid becoming victims. Women can prevent cybercrimes against themselves by adhering to certain best practices.

- **Maintain the Privacy**

When sharing personal information online, especially on social media, use caution. Don't publicly disclose your home address, phone number, or other private information. Phishing emails and phone calls requesting personal information should also be avoided.

- **Two-Factor Authentication**

After providing an additional form of verification, such a code texted to your phone, in addition to your password, two-factor authentication strengthens the security of your online accounts. Numerous well-known internet businesses, such as social networking sites and email providers, provide this function.

- **Handle Social Media Cautionably**

Social media may have both positive and negative effects. Although it might facilitate communication with loved ones, it can also serve as a breeding ground for online criminal activity. [11]Be careful who you add as pals, and refrain from posting private or delicate images online.

- **Secure Passwords**

Passwords consist of a combination of capital and lowercase letters, numbers, and special

[10] https://www.ijfans.org/uploads/paper/374cf990d6568e78319acc782da11df2.pdf

[11] Gupta, S., & Kapoor, M. (2018). Cyber Crime in India: An Empirical Study on Cyber Crime Awareness among Women. International Journal of Management Studies, 5(4), 106-111. Retrieved from http://www.aarf.asia/images/short_pdf/1538513964_12.%20PAPER%203

characters and are at least 12 characters long. Don't use passwords that are simple to figure out, such as your name, birthdate, or pet's name.

- **Maintain Up-to-Date Software**

Maintain the most recent versions of all your software, including your operating system and antivirus program. Security patches that fix flaws that hackers may exploit are frequently included in software upgrades.

- **Antivirus Software**

Malware and other harmful software may be detected and prevented from infecting your device with the use of antivirus software. Installing trustworthy antivirus software and keeping it updated are important.

- **Report Incidents**

It's imperative that you notify the authorities if you fall victim to cybercrime. By reporting events, law enforcement may find and apprehend cybercriminals and help prevent future crimes.

VI. CONCLUSION

In recent years, cybercrimes against women in India have increased in number. The Indian government has launched a number of programs and put laws in place to stop and report cybercrimes against women in an effort to address this problem. Nonetheless, it is imperative to address the root causes of these crimes, which include patriarchal views, gender-based abuse, and a lack of knowledge about cyber security. [12]Women must take preventative actions, including as making secure passwords, exercising caution when disclosing private information online, and quickly reporting incidences to the appropriate authorities. Campaigns for awareness and educational initiatives may be extremely important in equipping women with the information and abilities they need to defend themselves against online threats. In conclusion, cybercrimes against women in India are a severe problem that calls for coordinated action from the government, law enforcement, IT sector, and general public in order to be successfully addressed. We can establish a safe and secure online environment for Indian women if we work together and take the appropriate approach.

*****

[12] United Kingdom Home Office. (2019). Cyber crime: Understanding the online offender. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/ cyber-offender-understanding.pdf