Page 2237 - 2245 **DOI:** *https://doij.org/10.10000/IJLMH.119271*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Cyber Crime against Women in India Cyber Crimes: Types, Patterns and Prospects

S.A. SUBHA SHREE[1]

ABSTRACT

There are various crimes against women in India, in cybercrime is one among them. Cybercrime is any criminal activity involving a computer/Mobile as the target or tool of the crime. According to the data released by the National Crime Records Bureau(NCRB), the number of cybercrime incidents in 2021 has gone up by 18.4 % since 2019, but the number of such cases against women has risen by a significantly steeper 28 %. This society is equally balanced with men and women, but women are targeted the most in this cybercrime. Though women are treated as goddesses, they are also easily trapped as victims in this crime network. Both educated and uneducated women are unaware of this cybercrime. There are various cybercrime cases in India against women. Indian women are not able to report cybercrime immediately as they are not aware and do not want to face it. Even though there are various legislations and authorities to prevent cybercrime, social awareness among women is essential to prevent such crimes. I have analyzed the reason for the growth of cybercrimes, types, impact, and possible remedy. I have also discussed the major cybercrimes against women.

Keywords*: Cybercrime, Growth of cybercrime, Crime against women, social awareness.*

I. INTRODUCTION

The more the technology is developed the crimes are increasing nowadays. In the present culture, there is no one without a computer and smart phone. People consider that having a mobile in their hand is like grabbing the whole world at their finger tip. This is partially acceptable until they are safe from the hands of hackers. All the countries are facing this cybercrime issue, including India.

The issues related to Cybercrime and electronic commerce are mentioned in the Information Technology Act 2000, which was amended in 2008. The first cybercrime occurred in 1992 when the first polymorphic virus was released in India. The case of Yahoo v. Akash Arora (1999) was one of the earliest examples of cybercrime in India. A permanent injunction was sought out in the case of Akash Arora in which he was accused of using the domain name

[1] Author is a LLM student at School of Excellence in Law ,Chennai, India.

 [ISSN 2581-5369]

'yahooindia.com'. We all know that due to the COVID-19 pandemic, every person has to stay at home and depend only on mobile phones for communication. Even children are forced to use mobile phones during their academic year. Due to this, cyber-crime cases increased by 11.8% in 2020. Cybercrime cases against women have increased by 24%, and cases against children have increased by 261%, according to *Crime in India – Statistics Volume II* by the National Crime Records Bureau (NCRB).

Data showed that 10,730 incidents, or 20.2% of the 52,974 incidents registered in 2021, were reported as crimes against women. The major question is why there is an increased cybercrime case against women than men? There are various answers to this single question. But the first and foremost answer is that it is due to the unaware of social Awareness for women. As compared to 2019, eight among the 28 states recorded a decline in cybercrime incidents in 2021. Among all states, Uttar Pradesh shows a decline of 22.7 percent in cybercrimes, whereas Karnataka shows a decline of 32.3 percent[2]. This does not mean that cybercrime will be destroyed in the future. Hackers are finding various methods to commit this crime.

(A) Literature Review

I have provided an overview of cybercrime against women in India by highlighting various types of cybercrime, which includes both sexual and non-sexual crimes. Various patterns of crimes are also analysed here and along with the prospects of the crime in the future. I have also provided punishments for such crimes along with their sections from the Information Technology Act 2008 and the Indian Penal Code (IPC). Some of the possible control measures have also been provided. Recent cases have been discussed to understand the nature of crimes up to date.

II. REASONS FOR THE GROWTH OF CYBER CRIME IN INDIA

Cybercrime is considered as one of the easy ways of earning money by the persons who is well knowledge in computed field and yet not having proper job. Some hackers even have a good job they involve in such crime for earning more money. Cybercrime is not only limited to big cities but also targeted at non-metros cities like Jalalpur in the northern state of Uttar Pradesh, Bhubaneshwar in eastern Odisha, and Patna in northern Bihar, according to the recent report by Pune-based antivirus from Quick Heal 2019. Mumbai ranked topmost, followed by New-Delhi.[3]

[2] Cybercrime Against Women, https://www.clearias.com/cybercrime-against-women/

[3] Lawsisto (no date) *Reasons for the growth of Cyber Crime in India: Lawsisto Legal News*, *REASONS FOR THE GROWTH OF CYBER CRIME IN INDIA | Lawsisto Legal News*. Available at: https://www.lawsisto.com/legalnewsread/NjY5NA==/REASONS-FOR-THE-GROWTH-OF-CYBER-CRIME-IN-INDIA (Accessed: 10 April 2025).

State of Tamil Nadu vs. Suhas Katti is considered one of the first cases to be booked under the Information Technology Act, 2000 (IT Act); the accused, Katti, posted obscene, defamatory messages about a divorced woman in the Yahoo message group. The accused was convicted under sections 469, 509 of the Indian Penal Code (IPC) and 67 of the IT Act 2000 and was sentenced to undergo 2 years of rigorous imprisonment and a fine (India News, 2010).

The criminal first targets the person. Open accounts such as Instagram, Facebook, etc., become their primary platform in which the criminals view all our posts and gather our information easily. They try to attack us by creating fake accounts and making us believe them blindly. Then, by their trick of sending some links as a gift, they hack our mobile easily. Some coupons, bank offers, lottery etc., attracts people a lot[4]. These are all the tricks they follow to fall into their trap. Mostly housewives, young girls, and children are prone to such traps. Online fraudsters can operate anywhere around the world, which is one of their plus point.

Maharashtra Deputy Chief Minister Devendra Fadnavis said on Friday said Mumbai witnessed a 70 percent rise in cybercrime cases in 2022 compared to the previous year. [5]Two women software professionals from Hyderabad have become victims of the newest fraud in separate cases. While one lost Rs. 4.50 lakh, another was duped of Rs. 1.50 lakh. This is a very recent case that proves that people are not still aware of such crimes and easily get trapped. In the case of Onlyfans (2021), the women who subscribed to that page got hacked, and their private photos were leaked without their consent. In the" BulliBai app case" (2022), three persons were arrested for the fake auction of muslim women in India[6].

(A) Types of cybercrimes against women

The following are the types of cybercrimes against women in India.

1. Cyberstalking: This involves repeated harassment and intimidation through online platforms, such as social media or email.

2. Online harassment: This includes sending threatening or abusive messages, comments, or posts on social media or other digital platforms.

[4] Sjouwerman, S. (2024) *Seven reasons for cybercrime's meteoric growth*, *Forbes*. Available at: https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/?sh=464d58ca5fa2 (Accessed: 10 April 2025).
[5] Pti (2023) *Mumbai saw 70 per cent rise in Cyber Crime Cases in 2022: Devendra Fadnavis*, *Mid*. Available at: https://www.mid-day.com/mumbai/mumbai-news/article/mumbai-saw-70-per-cent-rise-in-cyber-crime-cases-in-2022-devendra-fadnavis-23273317 (Accessed: 10 April 2025).
[6] *Bulli Bai app: Three arrested for fake auction of Muslim women in India* (2022) *BBC News*. Available at: https://www.bbc.com/news/world-asia-india-59835674 (Accessed: 10 April 2025).

 [ISSN 2581-5369]

3. Cyberbullying: This involves using digital platforms to harass, intimidate, or humiliate a woman or a girl.

4. Revenge porn: This involves the non-consensual sharing of intimate or sexual images or videos online, often to shame or embarrass the victim.

5. Identity theft: Women are at risk of having their personal information stolen and used for fraudulent purposes, such as opening bank accounts or taking out loans in their name.

6. Financial fraud: Women are often targeted with phishing scams and other types of financial fraud, which can result in significant financial losses.

7. Online grooming: Predators use social media and other online platforms to target and groom young girls and women for sexual exploitation.

8. Cybercrime related to matrimonial and dating sites: Women can fall prey to fraudulent online matrimonial and dating sites, where they may be subjected to blackmail, extortion, and other forms of exploitation.

(B) Patterns And Prospects of Cyber Crime

Cybercrime is an ever-evolving field, and new patterns of criminal behaviour and attacks emerge constantly, such as,

1. Phishing: Phishing attacks involve creating fake emails or websites that are designed to trick users into revealing sensitive information such as passwords or credit card details.
2. Ransomware: Ransomware is a type of malware that encrypts files on a victim's computer or network, making them inaccessible until a ransom is paid.
3. Social engineering: Social engineering attacks involve tricking people into revealing sensitive information or performing actions that benefit the attacker.
4. DDoS attacks: Distributed denial-of-service (DDoS) attacks involve flooding a website or server with traffic, causing it to become unavailable.
5. Malware: Malware is software that is designed to harm or gain unauthorized access to a computer system. It can be spread through emails, infected websites, or file downloads. Mumbai ranked topmost in such crime.
6. Advanced persistent threats (APTs): APTs are attacks that are designed to penetrate a system and remain undetected for an extended period, often using sophisticated techniques such as zero-day exploits.

 [ISSN 2581-5369]

7. Insider threats: Insider threats involve attacks by people within an organization who have authorized access to systems and data.
8. Botnets: Botnets are networks of compromised computers that can be controlled remotely and used to carry out attacks such as DDoS attacks or spam campaigns.
9. E-commerce fraud: E-commerce fraud involves using stolen credit card information or fake accounts to make fraudulent purchases online.
10. Identity theft: Identity theft involves stealing personal information such as social security numbers or credit card details, which can then be used for fraudulent purposes.

Increased sophistication, Greater frequency, increased financial losses, Greater complexity, Targeted attacks, emerging threats, and Transnational nature are some of the prospects of cybercrime in India. Overall, the prospects of cybercrime suggest that it will continue to be a significant threat in the years to come. Individuals, businesses, and governments need to be vigilant and take steps to protect themselves against these risks.

III. LEGAL PROTECTION OF WOMEN FROM CYBER CRIMES

The Information Technology Act (amended)2008 has recognised various sexual offences and non-sexual offences against women in India.

I have analysed various crimes such as Offensive communication, Offences Against Cyber Privacy, Hacking, Stalking, and Related Crimes. They are all grouped under non-sexual offences. Now, let's discuss them one by one.

(A) Non-Sexual Offences

a. Offensive Communication

Offensive communication is generally used in public networks and chatting sites. Apart from using English slang words towards women in open public forums, it has become a 'fashion' to use colloquial vernacular slang for attacking women.

Such offensive communications are compactly regulated by section 66A of the Information Technology Act (amended), 2008, which includes grossly offensive communications, information containing menacing character, defamatory statements which the sender knows to be false, but are communicated to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will etc. Section 66A prescribes 3 years imprisonment or a fine for such offensive communications. In practice, the IPC is also applied to book the offender under Section 500, which prescribes punishment for defamation with

simple imprisonment, which may extend to two years or with a fine or with both. Section 502 (b) of the IPC prohibits the sale of printed or engraved substance containing defamatory matter, knowing it to contain such matter in any other case, and terms it as a non-cognizable offence with simple imprisonment for 2 years or with a fine or with both. Section 509 of the IPC covers an intention to insult the modesty of a woman.

b. Offences Against Cyber Privacy, Hacking, Stalking, And Related Crimes

In the case of Kharak Singh vs. State of UP[7] by the Supreme Court of India expanded the meaning of "life" to cover privacy as a basic fundamental need to enjoy life: "By the term life as used here, something more is meant than mere animal existence. However, this right is very much interrelated with the right to live with human dignity. In the case of Maneka Gandhi vs. Union of India[8], the court held that: "right to live is not merely confined to physical existence, but it includes within its ambit the right to live with human dignity". Hence, through the above two cases, it is found that privacy is concerned with human dignity, and the offences against cyber privacy should be punished. Section 43 of the IT Act, 2008 regulates the right to unauthorized access of computer data. Section 65 further prohibits tampering or modification of such data that were accessed unauthorized. When we feel that our account was taken over or misused, section 66C of IT 2008 punishes the Criminal with imprisonment of 3 years or with a fine of 1 lakh rupees. Section 72 of the IT Act could be stretched to cover stalking menaces. This section states that when a person without another person's consent discloses his/her electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. Section 509 of the Indian Penal Code may also be pulled in to cover online stalking.

(B) Sexual Offences

a. Voyeurism

Section 66E of the Information Technology Act, 2008 says that Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Section 67A may also be used to prohibit such voyeur sexual activities, as the wordings of Section 67A strongly prohibit the distribution of sexually explicit acts or conduct.

[7] Kharak Singh vs. State of UP , AIR 1963, SC 1295
[8] Maneka Gandhi vs. Union of India , AIR 1981, SC 746

 [ISSN 2581-5369]

b. Pornography, Obscenity, And Indecent Representation of Women In Cyberspace

Section 67 deals with internet obscenity, and 67A is internet pornography of the Information Technology Act, 2000 (amended in 2008). Both offences deal with the indecent representation of women in cyberspace. The punishment for internet obscenity is imprisonment for 2 to 3 years or a fine up to 5 lakhs. The punishment for internet pornography is imprisonment that may extend to 5 years and a fine up to 10 lakh.

c. Control of cyber crime against women in India

Raising awareness among women about the various types of cybercrimes and how to prevent them is critical. This can be done through workshops, seminars, and campaigns. Women should be taught digital literacy, including how to use the internet safely and securely. This can help them understand the risks associated with online activities and take preventive measures. The government should consider enacting stronger laws to protect women from cybercrime. This would include provisions for harsher punishments for offenders, as well as measures to improve the investigation and prosecution of cybercrime cases. It's important to have a reliable reporting mechanism in place for women who are victims of cybercrime. This can include helplines, email addresses, and online complaint portals. The government can also create a dedicated cybercrime cell to handle such cases. The development of technology solutions such as cybersecurity tools, software, and applications can help prevent cybercrime against women. It is essential to have technologies like two-factor authentication, encryption, and firewalls. Women should be cautious about sharing their personal information online. They should be advised to keep their social media profiles private, avoid sharing sensitive information online, and be cautious when clicking on links or downloading files. We should not fall for phishing click baits (messages/emails from unknown senders, prizes, bonuses, etc.). We must choose cash on Delivery (COD) if we are not sure of the online payment. If bank fraud is suspected, we must immediately complain to the respected bank manager and block the account. We can file an FIR. We can file a cyber complaint at - National Cyber-crime reporting portal https://cybercrime.gov.in/.We also have the National Commission for Women (NCW) – registering complaints through emails (complaintcell-ncw@nic.in).CyberCrime Prevention against Women and Children (CCPWC) spreads awareness against cybercrimes. The Government has established the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs to provide a framework and ecosystem for LEAs to deal with cybercrimes in a comprehensive and coordinated manner. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, empower the users of

 [ISSN 2581-5369]

Intermediaries and make the social media platforms accountable for their safety. In case of serious cybercrime, the victim can file a complaint at the nearest cybercrime police station. Women can also call the Women's Helpline number (181) to report cybercrime against them. This helpline is available 24/7.

IV. CONCLUSION

The first and foremost thing I would like to suggest is that women should have the braveness to face the problem and share with their family members against such crimes. The centre and state should bring new legislation against this cybercrime. In conclusion, cybercrime against women in India is a growing problem that has serious implications for women's safety and well-being in the digital space. It is essential to prioritize the safety and well-being of women in the digital space and work towards creating a more inclusive and equitable society where women can exercise their rights without fear of harassment or violence.

*****

 [ISSN 2581-5369]

V. REFERENCES

- "Cyber Crimes against Women in India," by Dr. Ritu Sharma, published in 2019
- "Women and Cybercrime in India: Challenges and Solutions," edited by Dr. Debarati Halder and Dr. K. Jaishankar, published in 2017
- C. Burgess-Proctor, "Understanding the Malevolent Use of Technology by Intimate Partner Abusers," Violence Against Women, vol. 21, no. 8, pp. 995-1016, 2015.

*****