Digital Object Identifier: 10.48165/iitmjit.2025.11.1.8

Legal Tackling of Cyber Crimes against Women in Prison

[1]Astha Bhatnagar, [2]Shewta Thakur
[1,2]Galgotias University
[1]asthaab716@gmail.com

Abstract: Cybercrimes against women have emerged as a critical issue in the digital era, with offenses like extortion, phishing, cyber stalking, and cyber defamation becoming increasingly common. This paper delves into the various forms of cybercrimes targeting women and evaluates the legal mechanisms designed to protect them. It examines key provisions of the Indian Penal Code, 1860, and the Information Technology Act, 2000, which address crimes such as sexual harassment, voyeurism, stalking, and identity theft. Additionally, the paper highlights significant judicial rulings that have influenced the legal framework for combating cybercrimes against women in India. By analyzing these legal provisions and landmark judgments, this study seeks to contribute to the development of more effective strategies for safeguarding women in the digital space.

Keywords: Cyber bullying, Cyber Crime, Information Technology Act, Phishing, Sextortion

1. Introduction

Cybercrime has become a pressing concern in the modern era, with women being among the most vulnerable targets. Cybercrimes refer to offenses committed through electronic communication or information systems, involving illegal activities where computers and networks play a central role. With the rapid expansion of the internet, the prevalence of cybercrimes has also surged, as criminals no longer require physical presence to commit offenses. In response to this growing threat, cyber laws were established to regulate and control crimes carried out via the internet, cyberspace, or digital resources. Cyber law encompasses legal issues related to the use of communication and computer technology, playing a crucial role in the digital age by governing online activities and transactions.

According to the National Crime Records Bureau (NCRB), 52,974 cases of cybercrime were registered, marking a 5.9% increase from 2020 (50,035 cases). The crime rate in this category rose from 3.7 in 2020 to 3.9 in 2021. In 2023, 60.8% of cybercrime cases were linked to fraud (32,230 out of 52,974 cases), followed by sexual exploitation at 8.6% (4,555 cases) and extortion at 5.4% (2,883 cases). The NCRB data for 2021 also revealed a more than 40% rise in crimes against women and children, a charge-sheeting rate of just 31% for IPC cases, and a staggering 111% increase in cybercrime cases in the national capital.

2. Types of Cyber Crimes Against Women

2.1 Sextortion: One of the most prevalent cybercrimes against women, even during the pandemic, was sextortion. Offenders blackmailed victims using their private or manipulated images, demanding money or sexual favors. Many perpetrators, frustrated by financial constraints, resorted to threats, coercing victims into engaging in video calls or exchanging explicit messages**.**

2.2 Phishing: Phishing is a fraudulent practice where an individual or entity impersonates a trusted organization in electronic communications, such as emails or messages, to deceive victims into revealing sensitive information like passwords and credit card details. It is a widespread form of cybercrime used to exploit personal and financial data**.**

2.3 Cyber Obscenity/Pornography: Considered one of the most severe online offenses, cyber obscenity involves the publication or distribution of pornographic content through electronic means. This includes the unauthorized dissemination of explicit material that violates privacy and dignity**.**

2.4 Cyber stalking: Women are often the primary targets of cyber stalking, a digital extension of traditional stalking. The Oxford Dictionary defines stalking as covertly pursuing someone. Cyber stalking includes tracking a person's online activities, sending persistent or threatening emails, posting messages on forums they frequent, or infiltrating their digital spaces. This crime leverages technology to harass and intimidate victims.

3. Legal Measures to Protect Women from Cybercrimes

Although there is no dedicated legal framework exclusively governing cybercrimes against women, several provisions across different laws offer legal recourse.

3.1 The Indian Penal Code (IPC), 1860

Before 2013, cyber bullying and online crimes against women were not directly addressed under the law. However, the **Criminal Law (Amendment) Act, 2013**, introduced Sections **354A to 354D** to tackle such offenses:

- **Sexual Harassment (Section 354A):**
- Covers acts such as demanding sexual favors, showing pornography without consent, or making sexually inappropriate remarks.
- Punishable by up to **three years of imprisonment, a fine, or both**.
- Less severe offenses carry penalties of up to **one year of imprisonment, a fine, or both**.

- **Voyeurism (Section 354C):**
- Defined as capturing or distributing images of a woman engaged in a private act without her consent.
- Conviction results in **up to three years of imprisonment for the first offense** and **up to seven years for repeat offenses**.

- **Stalking (Section 354D):**
- Covers both physical and online stalking, including persistently pursuing a woman despite her disinterest or monitoring her online activity.
- Punishable by **up to three years of imprisonment and a fine**, increasing to **five years for repeat offenses**.

- **Other Relevant Legal Provisions**

Beyond specific amendments, other sections of the IPC provide avenues for prosecuting cybercriminals:

- **Defamation (Section 499 & 500):**
- Intentionally harming someone's reputation through false statements or images.
- Punishable by **up to two years of imprisonment, a fine, or both**.

- **Criminal Intimidation (Section 503):**
- Threatening someone to manipulate or control their actions, often seen in cyber blackmail cases.

- **Anonymous Criminal Intimidation (Section 507):**
- Addresses threats made anonymously through digital means, providing for strict penalties.

- **Insulting a Woman's Modesty (Section 509):**
- Covers verbal remarks, gestures, or online content intended to offend or violate a woman's dignity.
- Offenders can face **up to three years of imprisonment and a fine**.

By enforcing these laws and raising awareness, stronger legal mechanisms can help curb cybercrimes against women and ensure their safety in the digital world.

3.2 The Information Technology Act, 2000

In order to facilitate electronic filing of documents with government agencies, this Act[16] was passed in 2000 to give legal recognition to transactions conducted through electronic data interchange and other electronic communication methods, also known as electronic commerce. These transactions incorporate the use of alternatives to paper-based methods of communication and information storage.

- **Offence of Identity Theft**: According to Section 66C of the IT Act, identity theft is a crime that carries penalties. This clause would apply to cyber hacking situations. This provision stipulates that anyone who dishonestly or fraudulently uses another person's password, electronic signature, or other unique identifying information faces a maximum sentence of three years in prison and a fine of up to Rs. one lakh.
- **Violation of Privacy:** Section 66E deals with situations in which someone's right to privacy is violated. Taking, sharing, or sending a picture of someone's private area without their permission or in a way that infringes on

their privacy can result in up to three years in prison and/or a fine.

➢ **Publishing or transmitting obscene material in electronic form:** Section 67, which prohibits the publication, transmission, or distribution of pornographic material, carries a maximum penalty of three years in prison or a fine for a first offense and up to five years in prison or a fine for a second.

➢ **Publishing or transmitting of material containing sexually explicit act, etc., in electronic form:** Section 67A defines publishing, transmitting, or assisting in the transfer of sexually explicit material as a misdemeanour, which carries a maximum sentence of five years in prison and a fine for a first conviction and a maximum sentence of seven years in prison and a fine for a subsequent conviction.

3.3 The Indecent Representation of Women Bill, 2012

Obscene depictions of women in publications, advertising, and other media are prohibited by this Bill. With the passage of this bill, the legal framework will be expanded to cover electronic and audio-visual media, as well as the distribution of information online and the representation of women on the internet. But as of July 2021, this Bill has been withdrawn.

4. Role of Indian Judiciary

The Indian judiciary has played a significant role in addressing cybercrime against women by delivering several landmark judgments. Some of these cases are highlighted below:

Ritu Kohli Case: The **Ritu Kohli Case** was India's first reported instance of **cyber stalking**. Mrs. Ritu Kohli filed a complaint with the police, stating that an individual was impersonating her online on for four consecutive days, primarily in the **Delhi Channel**. The impersonator used her name, shared her address, and engaged in inappropriate conversations. Furthermore, the individual intentionally provided her phone number to other chat participants, encouraging them to call her at odd hours.

As a result, Mrs. Kohli received nearly **40 calls** within three days, significantly disrupting her personal life. Following an investigation, the police traced the **IP addresses**, conducted a thorough inquiry, and arrested the offender. A case was filed under **Section 509 of the Indian Penal Code (IPC)**, but the accused was later released on bail. This case marked **India's first official report of cyber stalking**.

Cyber stalking, much like email harassment, is not explicitly addressed under existing **cyber laws in India**. However, such offenses can be prosecuted under:

- **Section 72 of the Information Technology (IT) Act, 2000** – for breach of confidentiality and privacy.
- **Section 441 IPC** – for criminal trespass.
- **Section 509 IPC** – for outraging a woman's modesty.

This case set a precedent for recognizing **cyber stalking as a punishable offense**, highlighting the need for stronger legal provisions to tackle digital crimes.

In case of ***Avnish Bajaj* v. *State (N.C.T.) of Delhi***[1], Bazee.com a customer to customer website was caught selling MMS videos in the name "DPS girls having fun". Vanish bajaj CEO of the sales company was arrested and was his bail plea was rejected. He was arrested under section 67 of the Information Technology Act, 2000. In this case, the defendants claimed section 67 of Information Technology Act, 2000 relates to publication of obscene material not transmission of it. The court held that actual obscene recording/clip could not be viewed on the portal of Baazee.com.

A Chennai court rendered a decision in State of Tamil Nadu v. Suhas Katti[2] in 2004. After declining a man's marriage proposal, the divorced woman complained to the police about him sending her offensive, defamatory, and bothersome messages in a Yahoo message group. In order to forward emails received in the woman's name, the accused created a phony email account. People who thought the victim was soliciting for sex work also called her. After the police complaint was filed in February 2004, the Chennai Cyber Crime Cell was able to secure a conviction within seven months of the First Information Report being filed. Katti received two years of rigorous imprisonment and a fine of Rs. 500 for violating S. 469 IPC (forgery with the intent to damage one's reputation), one year of simple

imprisonment and Rs. 500 for violating S. 509 IPC (words, gestures, or acts meant to offend a woman's modesty), and two years of rigorous imprisonment and a fine of Rs. 4,000 for violating S. 67 of the IT Act 2000 (punishment for publishing or transmitting obscene material in electronic form).

In ***Shreya Singhal* v. *Union of India*** [2], this ruling, which relates to section 66A of the Information Technology Act of 2000, is historic. This section was not part of the Act when it was first passed, but it was made effective on October 27, 2009, by an Amendment Act of 2009. "A rapid increase in computer and internet use has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism, breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personating commonly known as Phishing, identity theft, and offensive messages through communication services," the Amendment Bill explains in its justification for the insertion of section 66A. Therefore, in order to prevent such crimes, penal provisions must be incorporated into the Indian Penal Code, the Indian Evidence Act, the Information Technology Act, and the Code of Criminal Procedure.

5. Analysis of Present Legal System

The rising number of crimes against women is a significant concern for any state, but cybercrimes pose an even greater challenge due to the anonymity the internet provides. Criminals can easily create fake identities and engage in illegal activities, making detection and prosecution difficult. To combat this, the government should implement stricter regulations for **Internet Service Providers (ISPs)**, as they have complete access to data being used by individuals online. ISPs should be required to report any suspicious activities, which would help in preventing cybercrimes at an early stage.

Additionally, **cyber cafes** should be subject to stricter regulations, ensuring they maintain detailed records of customers who use their internet services. Many individuals engage in cybercrimes from cyber cafes to mask their identities and avoid detection. Proper record-keeping would make it easier for law enforcement agencies to track and identify offenders.

Public awareness regarding **cyber safety and digital rights** is also crucial. Many internet users in India are unaware of their rights and legal protections in cyberspace. Efforts must be made to educate people on how to safeguard themselves against cyber threats and ensure responsible digital behavior.

One of the major obstacles in addressing cybercrimes against women lies in **procedural legal challenges**, including jurisdictional conflicts, lack of sufficient evidence, and an underprepared judiciary. The judiciary plays a crucial role in shaping legal frameworks to combat cybercrimes effectively. With the expansion of cyberspace, traditional territorial boundaries have become less relevant. The jurisdictional limitations under **Section 16 of the Code of Civil Procedure and Section 2 of the Indian Penal Code** may not be sufficient to address cyber-related offenses, necessitating alternative dispute resolution methods for effective enforcement.

6. Conclusion

Several laws have been enacted to address cybercrimes against women, but continuous efforts are needed to ensure that technological advancements are used for ethical and legal purposes rather than criminal activities. Policymakers, law enforcement agencies, women's rights activists, and social organizations must recognize that cyberspace is as serious an issue as any other societal problem.

India, with its vast internet user base, faces a high risk of cybercrimes. Monitoring such a large digital landscape is challenging, and the government must **strengthen cyber security measures** to keep up with rapid developments in data services and internet access. In today's world, **cyber security is as critical as national security**, and building physical defenses will be ineffective if the real battle is being fought in the digital space. While global concerns over nuclear warfare persist, **cyber warfare has become an even more immediate and pressing issue**. India must ensure that women are not subjected to further victimization in this ever-evolving digital landscape.

References

1. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India.

International Research Journal of Engineering and Technology (IRJET), *4*(6), 1633-1640.
2. Balhara, Y. P. S., Sarkar, S., & Rajguru, A. J. (2024). Drug-related offences in India: Observations and insights from the secondary analysis of the data from the National Crimes Record Bureau. *Indian Journal of Psychological Medicine*, *46*(6), 527-534.
3. Rattan, J., & Rattan, V. (2017). Cyber Laws & Information Technology. *47 Bharat law publishing, Calcutta,*
4. GustafsonRID="**" ID="**" Present address: Courant Institute, 251 Mercer St., New York, NY 10012, USA.¶ E-mail: gustaf@ cims. nyu. edu, S., & Sigal, I. M. (2000). The Stability of Magnetic VorticesRID="*" ID="*" Research on this paper was supported by NSERC under grant N7901. *Communications in Mathematical Physics*, *212*(2), 257-275.
5. Ter-Akopian, G. M., Hamilton, J. H., Oganessian, Y. T., Daniel, A. V., Kormicki, J., Ramayya, A. V., ... & Saladin, J. X. (1996). New Spontaneous Fission Mode for 252 Cf: Indication of Hyperdeformed 1 4 4, 1 4 5, 1 4 6 Ba at Scission. *Physical review letters*, *77*(1), 32.
6. Ter-Akopian, G. M., Hamilton, J. H., Oganessian, Y. T., Daniel, A. V., Kormicki, J., Ramayya, A. V., ... & Saladin, J. X. (1996). New Spontaneous Fission Mode for 252 Cf: Indication of Hyperdeformed 1 4 4, 1 4 5, 1 4 6 Ba at Scission. *Physical review letters*, *77*(1), 32.
7. Law, U. (2009). *Indian Penal Code*. Universal Law Publishing.
8. Kushwah, J. P. (2021). Practical Approach towards Law Relating to Sexual Offences in perspective view of the Criminal Law (Amendment) Act, 2013. *Research Inspiration*, *7*(I), 15-23.
9. Dixit, V. A. I. B. H. A. V., & Singh, S. H. R. E. Y. (2013). The Criminal Law (Amendment) Bill, 2013-a Critical Analysis'. *Rostrum's Law Review*.
10. Kaur, D. R., & Aggarwal, D. R. A. (2013). The information technology act, 2000-demystified with reference to cybercrimes. *Paradigm*, *17*(1-2), 99-104.