International Journal of Social Science Research and Review

ijssrr.com
editor@ijssrr.com
Volume 9, Issue 11
November 2026
pp. 14–20

An Exploratory Study on the Implementation of Cyber Laws that aim at Protection of Women against Harassment in India

Ayaana Gaggar
Modern School Vasant Vihar, New Delhi, India
gauravgaggar@gmail.com

DOI: https://doi.org/10.47814/ynkg0c44

Abstract

The paper analyses the extent of cybercrimes that have been increasingly committed against the population and especially women. One of the reasons for this increase is the widespread use of the internet and the large quantities of smartphones in existence. Both of the above are available to the majority of the population primarily due to access to inexpensive data and cheap smartphones. The government has made great inroads in trying to track the perpetrators of crime as well as announcing publicly the types of criminal cybercrime activities that are being committed. In fact, the government has gone a step further and made the banks responsible for any large transaction that may occur in the accounts of the elderly and female gender. In addition, the banks have also put stringent checks to try and stem the increasing incidents of cybercrime. In its recent regulation, the government has decided to disperse a marginal amount of money towards victims of cybercrimes. But in the end, it is the public at large and the continued adoption of advanced AI technology that can prevent criminals from extracting large sums of money.

Keywords: *Cybercrime; Cyber Harassment; Women Safety; Deepfakes; Information Technology Act; Digital Fraud; Cyber Law Enforcement*

Introduction

The internet has fundamentally altered the way people communicate, work, and navigate their daily lives. In India, this transformation has been particularly dramatic. With over 750 million internet users and smartphone penetration reaching even the most remote corners of the country, cyberspace has become an inseparable part of modern existence. But alongside the opportunities this digital expansion brings, it has also opened the door to a disturbing range of criminal behaviours, many of which disproportionately target women.

To understand the problem at hand, it is first necessary to understand what cyberspace actually is. At its most basic, 'cyber' refers to anything relating to or involving computers, digital networks, and the internet. Cyberspace, as a concept, describes the *virtual environment in which digital communication and interaction take place* — a borderless, largely anonymous space where individuals, institutions, and governments converge. It is not a physical place one can point to on a map, yet its consequences are deeply real. What happens online is not to stay online. It spills into careers, mental health, relationships, and physical safety.

Cybercrime, broadly speaking, refers to any criminal activity that is carried out using a computer, a digital device, or a network. This can range from financial fraud and identity theft to hacking, data breaches, and the spread of malicious software. However, what makes cybercrime particularly difficult to pin down, legally and academically, *is that there is no single universally accepted definition of it.* Different countries, institutions, and researchers define it differently, and this inconsistency has real consequences for how such crimes are investigated, prosecuted, and understood. In the Indian context, cybercrime is primarily governed by the Information Technology Act, 2000, which has been amended over the years to keep pace with technological developments, though critics argue it still falls short in several critical areas.

Within the broader category of cybercrime, cyber harassment occupies a space that is at once deeply personal and systemically ignored. Harassment, in its conventional sense, *refers to unwanted behaviour that intimidates, humiliates, or threatens an individual.* When this behaviour migrates online, it takes on new and often more insidious forms. Cyber harassment against women includes online stalking, where perpetrators monitor a victim's

digital activity obsessively; cyberbullying, which involves repeated targeting through abusive messages or public humiliation; morphing, where photographs are manipulated and shared without consent; doxing, where personal information is published to incite others to cause harm; and the non-consensual sharing of intimate images, sometimes referred to colloquially as *revenge porn.*

These are not minor inconveniences. They cause lasting psychological damage, force women out of professional and public spaces, and in extreme cases, have driven victims to self-harm.

What makes cyber harassment particularly acute for women in India is the intersection of *gender inequality and digital anonymity*. The anonymity afforded by the internet emboldens perpetrators

who might otherwise be held socially accountable. Meanwhile, *deeply rooted cultural attitudes around gender, shame, and family honour discourage many women from coming forward.* When they do report, they frequently encounter law enforcement personnel who are either undertrained in handling cyber complaints or dismissive of their severity.

This study is born out of a recognition that the problem is not simply a legal one, nor simply a technological one — *it is social, institutional, and deeply gendered.* India has laws on paper. The question this research sets out to explore is *whether those laws are working in practice, for whom they are working, and what stands in the way of genuine protection for women navigating an increasingly hostile digital landscape.* Understanding where the system succeeds and where it fails is the first step toward building something better.

Literature Review

This research has indicated that cybercrime is not only enabled by technology but is inseparable from it. These are crimes that the existing legal systems were not equipped to handle.

Jurisdictional conflicts arise due to the internet not respecting such a system; perpetrators operate anonymously, and a large part of the harmful cyber activity falls outside the formally recognised definition of a criminal. This leaves victims without recourse and offenders without consequence. Cybercrime can be divided into two broad categories;

- A computer is a tool used to commit a recognisable offence such as harassment, blackmail, and fraud.
- A computer is not incidental to the crime; it is the crime. Hacking, unauthorised access and interference with digital systems all of these have no real equivalent in pre-digital law.

The mismatch between legal architecture and technological reality is where the most serious gaps in accountability continue to exist. [1]

Marngar, Abhinaya and Vismaya trace cybercrime from its earliest days, where isolated network intrusions by technically skilled individuals in the 1970s, to the current AI-driven offences. This trajectory happened gradually. With the spread of internet facilities in the 1990s, the shift towards crime followed. As a larger number of people used the facility, harassment cases increased. Social media gave perpetrators new reach and anonymity they had never had before. Women bore the sharpest end of this due to their lack of understanding of cybercrime. The use of deepfakes indicated that technology could fabricate intimate imagery, which is now possible even by ordinary people. Indian cyber legislation, much of it written before smartphones existed, was never designed for this reality. [2]

The Indian cyber law under the IT Act 2000, which was amended in 2008, was reactive from the start. It was built for a specific technological moment that has since passed. (The Section 66A). A provision meant to address online harassment was drafted so loosely that it ended up being used to silence dissent, until the Supreme Court struck it down in Shreya Singhal in 2015. Well-intentioned laws, but with poor drafting and unintended consequences, keeps occurring in the Indian scenario. As a result, women seeking protection are left navigating a legal framework that was never really built around their experiences. [3]

The Budapest Convention is the closest thing to a global standard, but its reach is un-even and India has not ratified it. The international framework consistently treats gender as secondary, prioritising instead data security and financial crime, indicating that harassment targeting women is a lesser problem, and national legislatures tend to reflect it. [4]

The authors believe that cybercrime has no single universal definition, as it represents a variety of offences with distinct motivations, techniques, and consequences. They suggest that there is more than one type of cybercrime, and it can be divided into many typologies to help lawmakers and policymakers better understand and respond to cybercrime. The research points to some crimes committed against computer systems and others that simply involve the use of digital technologies to commit traditional crimes. It is a conceptual distinction,

which is necessary for creating efficient laws and law enforcement policies, as well as for international cooperation.

The authors go on to stress the lack of consensus in terminology used by jurisdictions, which causes confusion, difficulty comparing data, prosecuting offenders, and cross-border investigations. *A unified definition and classification of cybercrime, thus, is essential to tackle the constantly changing cybercrime threat landscape.* [5]

Research gap and methodology

This paper will analyse the use of cybercrime in various areas in targeting women in general and Indian women in particular. What are the laws that the government has adopted to prevent the spread and address the intimidation by cybercriminals? How far have these laws been successful in preventing and spreading these crimes in the recent past?

The methodology adopted would be of the mixed-method type, which would include both quantitative and qualitative analysis. The quantitative data would be sourced from authentic government reports, and the qualitative explanation would also be from dependable government sources.

Analysis of existing laws and ordinances to prevent cyber harassment for women

Table 1; A comparative analysis of various laws over time

Year	Cybercrime against Women	Cybercrime against Women in India	Most Vulnerable Age Group
2021	Increased cyberstalking, cyberbullying, fake social media profiles, and image-based abuse after the COVID-19 digital shift.	Information Technology Act, 2000; IPC Sections 354A, 354C, 354D, 499–500, 509; National Cyber Crime Reporting Portal strengthened.	**18–30 years**
2022	NCRB data showed a substantial rise in cybercrimes against women compared with previous years, including cyberstalking and online harassment.	Enforcement of the IT Act, IPC, and Intermediary Guidelines & Digital Media Ethics Code Rules, 2021.	**18–30 years**
2023	Overall cybercrime cases in India increased by over 30%, cyber harassment of women also continued to rise with increasing use of	Bharatiya Nyaya Sanhita, 2023 enacted (replacing IPC 2000), retaining provisions relevant to stalking, voyeurism, criminal intimidation, and	**18–30 years**
	social media and digital payments.	**offences against women.**	
2024	NCRB reported another increase in overall cybercrime, while cyber offences targeting women—including sextortion, deepfakes, impersonation, and cyberstalking—remained a major concern.	Greater emphasis on platform accountability, cyber awareness campaigns, and specialised cyber police units.	**18–35 years**
2025	Cyber harassment became increasingly AI-enabled, with growth in deepfake images/videos, sextortion, and identity theft. The government strengthened awareness campaigns and cyber reporting mechanisms.	Implementation of BNS, IT Act, CERT-In directions, and expanded cybercrime reporting through I4C.	**18–35 years**

Source; EPW, Press Information Bureau, PRS Legislative Research, CJP, Drishti IAS, PRS, Legislative Research

Table 2; A comparative analysis of the percentage of women affected by cybercrime in the world and in India

Year	Most common crime against women	Percentage of women affected in the world	Percentage of women affected in India	Level of education of women affected
2021	Cyberstalking, online harassment, fake profiles	~38%	~27%	Higher secondary, **undergraduate and postgraduate students**
2022	Cyberstalking, image-based abuse, impersonation	~39%	~29%	College students and young professionals
2023	Sextortion, identity theft, cyberstalking	~40%	~31%	Undergraduate and postgraduate education
2024	*Deepfakes, sextortion, financial fraud, cyberbullying	~42%	~33%	University students and working professionals
2025	AI-generated deepfake abuse, sextortion, identity theft	~43%	~35%	Undergraduate, postgraduate and digitally active professionals

Source; National Crime Records Bureau, 2. Parliamentary Standing Committee on the Empowerment of Women (2026), 3. UN Women, 4. Norton Cyber Safety Insights Report (2021)

*Deepfakes became widespread across the world in 2024.

Laws and policies have been followed that have aided in the prevention of cybercrime.

India strengthens its laws and policies to combat cybercrime against women by criminalising online offences, protecting victims and enhancing cyber security, as internet access and digital platforms increase. Cyber stalking, identity theft, online harassment, image abuse, sextortion and sharing of private images have become rampant, and the government has responded by *developing a mix of laws, regulations, institutions and awareness measures to counter these crimes.*

The principal legislation governing cyber offences is the **Information Technology (IT) Act, 2000**, amended in 2008. The Act criminalises several cyber offences relevant to women, including identity theft (Section 66C), cheating by personation using computer resources (Section 66D), violation of privacy (Section 66E), and the publication or transmission of obscene or sexually explicit material in electronic form (Sections 67 and 67A). These provisions provide legal protection against offences such as fake social media accounts, online impersonation, revenge pornography, and the circulation of explicit content without consent.

In addition to the IT Act, the **Bharatiya Nyaya Sanhita (BNS), 2023**, which replaced the Indian Penal Code from July 2024, contains provisions relating to sexual harassment, stalking, voyeurism, criminal intimidation, extortion, and defamation. The **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023,** establishes procedures for investigating cyber offences, while the **Bharatiya Sakshya Adhiniyam (BSA), 2023,** recognises electronic records such as emails, text messages, social media posts, and digital photographs as admissible evidence in court, thereby strengthening prosecution.

The government has also introduced several policies and institutional measures. The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,** require social media platforms and digital intermediaries to remove unlawful content, appoint grievance officers, and cooperate with law enforcement agencies. The **Digital Personal Data Protection Act, 2023,** further protects individuals' personal information by regulating the collection and processing of digital data and imposing obligations on organisations to safeguard user privacy.

To strengthen enforcement, the Ministry of Home Affairs established the **Indian Cyber Crime Coordination Centre (I4C)** and launched the **National Cyber Crime Reporting Portal**, enabling victims to report cyber offences online. The **Cyber Crime Prevention against Women and Children (CCPWC) Scheme** supports specialised cyber police units, forensic laboratories, police training, and awareness campaigns to improve prevention and investigation. Together, these laws and policies have significantly enhanced India's

ability to prevent cybercrime against women, although continued legal reforms, stronger enforcement, and increased digital literacy remain essential to address emerging threats such as deepfakes and AI-enabled cyber abuse.

Reasons for the continuous growth of cybercrime especially against women

Deepfake Crime, Gender-Based Crime, and Financial Cybercrime can be considered as emerging problems for several reasons. First, the accessibility of advanced technologies such as artificial intelligence leads to a decreased level of expertise needed to perform cybercrime. For example, deepfake crime resulted in non-consensual imagery synthesis, election interference, voice cloning of family members, CEOs, and other individuals, face swapping for scams, and the use of celebrities' images for advertising. Second, the increased use of the Internet and smartphones allows perpetrators to find more victims and provides them with a greater number of ways to ensnare victims. For instance, gender-based cybercrime leads to cyberstalking, sexual harassment, revenge pornography, non-consensual distribution of sexual media, sextortion, gender-based trolling, doxxing, and cyber-enabled trafficking. The anonymity provided by the online environment encourages such criminal behaviour, while the lack of cybersecurity legislation and the possibility to operate across borders prevent detection, punishment, and accountability. Third, financial cybercrime is facilitated by the growing popularity of internet banking and online payment services. Examples of such crime include phishing, smishing, and vishing, business email compromise, card skimming and card-present scams, identity theft, cryptojacking, ransomware, counterfeit investment schemes and fraudulent Ponzi Schemes, ATM malware, and point-of-sale malware. Moreover, the problem is exacerbated by the fact that financial cybercrimes often go unreported by victims due to embarrassment (in case of gender-based cybercrime), lack of trust in institutions, or unawareness of being a victim (in the case of financial cybercrime). Finally, the ability to operate across borders makes many cybercrimes unpredictable, anonymous and challenging to control. In addition, using cryptocurrencies and other digital instruments makes it possible for perpetrators to avoid punishment and continue engaging in cybercrime.

The problem with financial and sexual crimes is the fear instilled in the victim of the widespread display of unsolicited photographs as well as the possibility of the targeted victims being those that may not have paid their financial dues to the government. As far as sexual crimes are concerned, the fear of being exposed and their positions in society prevent them from reaching out to the police. The fact that cybercriminals tend to target the elderly and the vulnerable also speaks of the aspirations of the perpetrators with regard to earning quick money.

Possible reasons to control the spread of cybercrime;

Advancements in detection technology, such as AI-powered deepfake detectors, fraud analytics software in the banking sector, and content moderation algorithms in social media platforms, have made it harder for cybercriminals to operate in these spheres anonymously. Effective moderation and the implementation of strict takedown policies by social media networks have reduced the traffic and popularity of deepfake and abusive content targeting women. In addition, increased awareness of the general audience regarding fake videos and the prevalence of fraudulent schemes has made users more cautious about sharing personal data online and clicking on suspicious links. Moreover, legislative changes such as specific laws criminalising intimate image abuse and cyberstalking and the creation of new crimes such as revenge porn and digital financial fraud have resulted in higher incarceration rates per cybercrime in many jurisdictions. Enhanced international collaboration through joint cybercrime units and the establishment of specialised investigation departments and victim support lines by Interpol, Europol, and national authorities has reduced repeat victimisation in several member states. The widespread advertisement that the government, banks and various fintech companies have unleashed in the public domain has increased awareness among all sections of society. They have addressed the manner in which frauds are used to dupe the public. Banks, in turn, have adopted extremely vigilant software that stops large sums of money from being transferred without additional consent of the account holder. The government of India has instituted a law where the bank is responsible for paying the account holder a fraction of the money that has been siphoned off through criminal means. Overall, the response to the cybercrime threat has demonstrated that despite the potential for exponential expansion of trying to prevent cybercrimes that have been aided by technology, effective legal means, societal awareness, the level of crime continues to increase.

Limitations of the data used

While this research draws on the most credible sources currently available, several limitations affect the reliability and completeness of the data used to assess the scale and impact of cybercrime.

Perhaps the most significant limitation is the recognised problem of underreporting. A significant percentage of cybercrime incidents are not reported to the authorities by their victims, either because they did not realise that

they were a victim of a crime or because they were embarrassed to do so. In addition, they might not have had faith that the police could do anything about it or, in case of a company, did not want to lose customers' trust and ruin the reputation. This results in a so-called 'dark figure' of crime, which represents a large disparity between the 'true' value of any given crime and the number actually recorded by the police. As a result, statistics collected for the purposes of the article might represent only a small percentage of all cybercrime incidents.

A further limitation is the very presentation of the data. Most of it only includes the numbers of incidents reported but does not differentiate between those that have been successful, partially interrupted, or completely foiled by counter-terrorist measures or preventative technology. This, clearly, poses a problem in determining the efficacy of a given strategy, police operation, or software based on success rates, as both successful and foiled attacks will be bunched together in statistics.

Due to the limitations of time and financial resources, the research relied on secondary data from various sources. Since the research is not based on primary data, there is a limitation that comes with using secondary data: a lack of control over how the data was gathered, defined, and categorised. Therefore, there could be inconsistencies between different countries or companies regarding what is considered a cybercrime.

The most vulnerable sections of society are the ones least likely to report crimes and are the most vulnerable, for example, women and the elderly, to becoming victims.

Further adding to the problem is that some individuals may become criminals themselves, unknowingly, for example, by allowing their bank account to serve as a vehicle for money laundering and thereby participating in criminal activity without realising it. As a result, the line between victim and criminal becomes blurred, which can lead to misclassification in official statistics.

Finally, it is essential to note that cybercrime is evidently more widespread in low-income countries, as they are less regulated and patrolled. It is also in developing countries that the level of digital literacy is the lowest, so their current assessment of the degree of cybercrime is presumably the most inaccurate.

Conclusion

This study aimed to evaluate the growing threat of cybercrime to women in India and assess whether legal and institutional measures in the country were adequate to the challenge. The research is based on the premise that India has a well-developed legal and institutional cyber security framework, represented by the National Cyber Security Policy, IT Act, 2000, the Bharatiya Nyaya Sanhita, 2023, I4C, the CCPWC Scheme, and the National Cyber Crime Reporting Portal. The problem is complicated by the fact that crimes occur at an increasing rate year after year due to people's inexperience with new information technologies and the relative accessibility of AI-based deepfake, sextortion, and voice-cloning software.

These issues cannot be solved by legal means alone, due to three basic problems, which are institutional barriers to the prevention of victimisation. Victims statements are under-recorded due to social stigma, family honour, and mistrust in the police, resulting in distortion of statistics. The speed of technological progress renders laws and their enforcement obsolete. The legislation is drafted in response to new technologies, not the other way around. Financial institutions and digital payment systems, due to their inability to detect wrong actions in accounts, have enabled criminals to continue targeting the vulnerable. Financial institutions should start moving towards full accountability.

What emerges as a key takeaway is that India needs to focus on amending the laws that relate to technology to ensure that the changes are future-orientated and more responsive to the evolving threats and challenges in the cyber world. There is a need to increase the rate of detection and moderation of such content through AI and invest more in creating awareness of such cybercrimes among the public. Moreover, there is a need to boost international cooperation, as cybercrimes are not geographical in nature. Unless these aspects are pursued, the changes to the current laws relating to technology in India will not be sufficient to protect women from cybercrimes in the long run.

Bibliography

1. Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things*, *19*, 100564. https://doi.org/10.1016/j.iot.2022.100564
2. Campbell, A. T., & Schwartz, M. (n.d.). ACM SIGCOMM Computer Communication Review. *ACM SIGCOMM Computer Communication Review*, *31*(5), 20–24. https://doi.org/10.1145/1037107.1037111

3. Bagree, C. (2023). Understanding the history of the internet, its regulation, and how the same is applicable to blockchain technology and its governance- Chirayu Bagree. *Ssrn*.
4. Kumar, R. (2014). Primer on Cyber Laws in India. *National Academy of Indian Railways*.
5. Marngar, R. A., Abhinaya, & SR, V. (2025). "Tracing The Evolution of Cyber Crimes: From Early Incidents to AI-Powered Threats and Their Impact" Rachel Ann Marngar, Abhinaya, Vismaya SR. *IJLTEMAS*.
6. Chowbe, V. S. (2011). An Introduction to Cyber Crime: General Considerations.

Research Gate.

7. Aprilia, C., Gebrewold, R. A., Bamiduro, M. D., & Borisova, N. (2026). The Evolution of Cybercrime and Its Impact on Various Sectors- Cindy Aprilia, Robel Amare Gebrewold, Mercy Damilola Bamiduro, Niurguiana Borisova. *Research Gate*.
8. Adel, A., & Norouzifard, M. (1996). Weaponization of the growing cybercrimes inside the dark Net: The question of detection and application. *Research Gate*.

[1] Vijaykumar Shrikrushna Chowbe
[2] Marngar, Abhinaya and Vismaya
[3] Rajnish Kumar
[4] Critical Analysis Of International Cyber Crimes By Vedica Saxena
[5] The book Conceptualising Cybercrime: Definitions, Typologies and Taxonomies. authored by Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken

9. Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Research Gate*.
10. PIB Delhi. (2024, February 7). *NCREASE IN CYBER CRIMES* [Press release].
11. Digital violence is intensifying, yet nearly half of the world's women and girls lack

legal protection from digital abuse. (2025). *UN Women*.

12. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.
13. Rai, D., & Bano, S. (2024, August 6). Cyber Police Stations and Cybercrime against Women in India.
14. Sriram, N. (n.d.). Standing Committee Report Summary Cyber Crimes and Cyber Safety of Women. *PRS Legislative Research*.
15. CJP Team. (2025). Cybercrime and the Crisis of Digital Justice: India's invisible

victims online. *CJP*.

16. *NCRB's Crime in India 2024 Report*. (2026). Drishti IAS; Drishti IAS.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (CC BY 4.0).