MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1624-1628

Cyberstalking Against Women in India: A Socio-Legal Analysis

Geeny Mourya[1*],
Research Scholar, Institute of Legal Studies and Research,
Mangalayatan University, Aligarh, U.P.
Email:bittu988@gmail.com.

Dr. Haider Ali[2],
Associate Professor, Institute of Legal Studies and Research,
Mangalayatan University, Aligarh, U.P.

Abstract:
Online harassment of women has become a notable instance of digital gender violence in India, which should be examined in a socio-legal analysis. This paper examines the rising rate of cyberstalking considering the current statistics provided by the National Crime Records Bureau, which shows that there is an extreme increase in cybercrimes cases, which portrays the vulnerability of women in the online environment. This paper examines the conceptual rationale and emerging aspect of cyberstalking, the difference between cyberstalking and traditional stalking and the major types of cyberstalking in Indian context. It also attempts a gendered examination to learn the psychological, social, legal consequences of such crimes by focusing on the overlapping between online hustle and actual violence. The study analyzes the legal structure that is currently in place, such as stipulations of the Information Technology Act, 2000, the Indian Penal Code, and the Bharatiya Nyaya Sanhita, 2023, and specifically, Section 78 BNS. It further assesses the judiciary role in developing cyberstalking jurisprudence and discusses some of the most important problems in reporting, investigation, and prosecution. Using the integration of both the legal analysis and the socio-cultural understanding, the study reveals gaps in the enforcement systems and victim protection systems. The paper also ends by offering recommendations that can be used to empower legal responses, institutional capacity and effective redressal to prevent cyberstalking of women in India.
Keywords: Cyberstalking, IT Act, Digital crime, Section 78 BNS, Judicial role.

INTRODUCTION

The continuously increasing number of cyberstalking of women throws a bigger investigation since its socio-legal consequences require the serious investigation of scholars. The report of the National Crime Records Bureau (NCRB) entitled Crime in India 2023 indicates that total cases of cybercrime against women in India had risen to 86,128 in 2023, as compared to 65,893 in 2022, which in turn reflects a 31.2% rise in reported cases, a matter that has been examined in this paper as a result of the multidimensional nature of cybercrimes against women in India. It aims at finding the special problems of the victims in the region and the effectiveness of the modern approaches to prevention, reporting and redressal. The psychological and social effects of cyberstalking upon women will be discussed, as well, and the analysis will focus on the fact that cyberstalking in many cases is related to real-life aggression.

The ubiquity of the online abuse of women and other marginalized genders in India points to a systemic problem in society that is far more than the initial pledge of a fair internet. In fact, digitalization of the society, especially at such a pace, has unknowingly left a door open to any sort of online abuse such as cyberstalking, harassment, and morphing, which severely undermines the dignity and safety of women. This is a rising international issue of concern especially in India where the rate at which internet penetration in the country has been rising has been matched by rising cyber-crime incidences of gender-based violence. This is also enhanced by the fact that perpetrators are allowed to be anonymous via the internet and in many cases, this increases the vulnerability of the victims and makes it difficult to investigate the case.

BACKGROUND OF CYBERSTALKING

The anonymity and mass use of the internet have placed India at the center in the statistics of sexual harassment worldwide (Singh and Gautam, 2022). As a second-largest internet user base in the world, the overlapping of the online and offline meeting has increased the levels of cyber harassment of women and made the issue more complex and widespread (Lal et al., 2024). This cyber space can tend to turn conventional stalking patterns into online actions, which includes the electronic track of movements, distribution of threatening messages, and flooding victims with unsolicited online content (AllahRakha, 2024). This change requires a re-analysis of the legal systems to accommodate the subtle forms of cyberstalking that cannot be confined to the traditional understanding of pursuits as physical but include continued online intrusion and mental coercion (Burrow et al., 2020). This type of digital violence may have a severe effect on the mental health of survivors, freedom of expression, mobility, and access to justice (Experiencing Technology-Facilitated Gender-Based Violence in India, 2025). This is a widespread problem that reflects those taking place in the global sphere, but women and other vulnerable populations are disproportionately impacted by it, causing severe psychological trauma, social isolation, and deprivation of a feeling of safety (Bezzina et al., 2025). The solution to this should be on the multi-pronged strategy that includes effective legal provisions, increase in digital literacy as well as supportive institutional mechanisms that are capable of countering the new approaches of cyberstalkers (Gurumurthy et al., 2019; Halder and Basu, 2024).

CYBERSTALKING IN INDIA: A GENERAL OVERVIEW

The rising access to the internet in India has not only brought related growth in cybercrimes but also women are often the main victims. This increased susceptibility is commonly explained by the anonymity cyberspace provides to criminals, allowing them to commit crimes between the harassment and abuse of others, as well as more sinister types of cyberstalking with no immediate fear of retaliation (Payne-James and Byard, 2023). A sophisticated type of online harassment, cyberstalking is associated with using digital tools and devices to hunt down and intimidate people using such techniques as unsolicited messages, monitoring social media usage, and online presence (Azam et al., 2023). This form of online anonymity does not only empower criminals but also poses a serious problem to the police in the hunt of criminals and in combining concrete evidence against them (Deo & Singh, 2022). Additionally, the technical difficulties linked to the jurisdictional aspects and retrieving user information of internet service providers are also another barrier to successful prosecution of cyberstalkers (Hedidi, 2023). The ignorance of the population and law enforcement towards the specifics of cyberstalking and other crimes prevents the possibility to respond quickly and efficiently, and it is the blind spot to consider the actual extent of the issue (Manjunath & S, 2024). The fast pace of technological advancement, as well as the nature of the internet itself, which is global by nature and anonymity that it provides, pose a serious challenge to effective regulation of cybercrime and its governance. Such obstacles are also enhanced by the fact that the jurisdictional issues, shortcomings in the publicity, and the lack of legislative coverage all worsen the ability to enforce the laws as well as preventive action (Kamarudin et al., 2025).

Cyberstalking is described as an act of following and harassing a person willfully, maliciously, repeatedly with the help of technology-related devices, computer-related devices, and digital resources, including email and social network (Kaur et al., 2020; Tjaden, 2013). It is defined by the consistent actions aimed at producing an apprehension and fear such as digital shadowing to collect data about a target (Halder, 2015; Tjaden, 2013).

Key characteristics and behaviors include:

Digital Pursuit: Repeatedly calling, chatting, or texting a victim despite being told to stop communicating with them, checking their online location or online activities (Halder, 2015).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1624-1628

Harassment and Threats: Sending spam or offensive or threatening messages, unwanted sexual advances, and sharing fake news or personal photos (e.g., defaming victims in chat rooms or pornography websites) (Halder, 2015; Tjaden, 2013).

Differences in Methodology: These are not the same as in physical stalking because in cyberstalking, the offender does not necessarily have to be near the victim, and can take advantage of the anonymity of the Internet to hide their identity and access a broader target base (Halder, 2015; Kaur et al., 2020; Tjaden, 2013).

Impact: The victim is likely to develop major psychological trauma, such as anxiety, fear, and a feeling of not being threatened in the moment, which becomes more pronounced over time (Halder, 2015; Kaur et al., 2020). Cyberstalking refers to cyber-victimization, which is a repeated unwanted mail or contact sent electronically to a person via the internet, email, social media, or other technology (Kaur et al., 2020). It is basically stalking or spying someone through the internet with the aim of collecting their personal data without their awareness with the aim of invading their privacy, harassing, terrorizing or intimidating them (Kavathekar & ILS Law College, Pune, 2021). In practice, cyberstalking is done by integrating the element of following somebody with a hostile purpose to inflict harm and then executed effectively, digitally (Halder, 2015). Academically, it encompasses a wide group of behaviors using information and communications technology, which can include the transmission of threats, false accusations, identity theft, data theft, and computer monitoring (Halder, 2015).

PRIMARY FORMS OF CYBERSTALKING

Cyberstalking is generally conducted through three primary methods:(Ogilvie, 2000)

- **Email Stalking:** This is a direct harassment in the form of unsolicited mails. It may involve hate mailing, sending obscene or threatening messages, computer viruses, or large amounts of electronic junk mail (spamming) in an effort to scare the victim.
- **Internet Stalking:** This is a more open and broad based form of stalking. A stalker can either trail a victim through websites or leave messages that are either fake or have been interfered with (like fake pornographic photos), or they can publicly publish personal information on the victim (i.e. address or phone number) to slander and/or threaten the victim. This type is especially threatening since it often overflows into physical and real-life stalking or even violence.
- **Computer Stalking:** This is a very intrusive technique that entails using the internet connections to be granted unauthorized access to the computer of the victim. The stalker will be able to interact with the target, steal the device, or get software to record keystroke and see the computer desktop in real-time.

DISTINCTIONS TO TRADITIONAL STALKING

Although cyberstalking is similar to offline stalking in that it is comprised of repeated actions that are intended to cause a feeling of apprehension and fear, it has some unique traits:

- **Absence of Physical Proximity:** A cyberstalker does not have to be physically close to the target; he or she is able to stalk someone living thousands of miles away.
- **Character of the Invasion:** Cyberstalking is based on technical invasion as opposed to physical invasion or violence.
- **Anonymity:** Technology enables cyberstalkers to easily distort or conceal their real identities and thus it becomes difficult to know who is monitoring an individual.
- **Sense of Threat:** Cyberstalking victims have the feeling of fear and intimidation slowly over time because there is an absence of perceived direct physical threatening nature, unlike the case in traditional stalking victims who have the immediate threat.

CYBERSTALKING AGAINST WOMEN: A GENDERED ANALYSIS

Women are particularly affected by cyberstalking, taking advantage of the gendered vulnerabilities and patriarchal power conditions of both cyber and realms (Udai and Sharma, 2025). Such gendered inequality is habitually associated with the social construct of social surveillance and control of women, which are further reinforced by the technology, which allows the perpetrators to carry their abusive actions into the internet (Marganski and Melander, 2021). Many cases of cyberstalking presuppose a first meeting in real-life scenarios, which means that this cyberbullying is often based on the existing relationships or face-to-face interaction (Panda, 2023). This digital-meets-physical harm highlights the need of intersectionality-based analytical framework, the analysis of how gender can dynamically intersect with age, socioeconomic status, geographical location and digital literacy, in order to impact the vulnerability of individuals to digital harm. This struggle usually takes the form of reputational assaults, falsified imagery, and threats to sexual violence, which serve as ways of silencing and social policing women, professionals, activists, and LGBTQ + (Harshit, 2025). This kind of digital violence is based on the ubiquity of the internet presence to cause emotional harm and social isolation, thus, violating the key right to privacy and online security (Jaishankar, 2016). Such recurrent digital violence generates a state of intimidation that limits the online presence and offline movement of victims, which makes it necessary to investigate further the sociotechnical roots of this phenomenon and consider it in relation to gender equality in the digital world (Laffier and Rehman, 2023; Miller, 2012). Moreover, the lack of strong legal frameworks that reasonably consider the complexities of online gender-based violence, as well as the globalization and generally borderless character of online interactions, makes it difficult to enforce the existing legislation and deliver the justice to the victims (AllahRakha, 2024a, 2024b).

LEGAL FRAMEWORKS ADDRESSING CYBERSTALKING

Since cyberstalking is transnational, both national legal tools and international law tools need to be explored to establish their effectiveness in offering redress and prevention. In particular, the application and enforcement of international law addressing technology-enabled violence against women has not yet been consistent because of the jurisdictional issues and the fast development of digital threats (Mythili & Nagamani, 2025; Rigotti, 2024). These complexities underscore the pressing need to have a unified global approach that will be able to harmonize national legislations and encourage international collaboration in effectively fighting technology based gender based violence. As an example, the definition of digital sexual harassment implies unwanted sexual advancements, remarks, or messages posted on the online platform, a type of gender-based violence that is often interconnected across different platforms to establish an abuse ecosystem (Basit et al., 2025). This can be cyberstalking, another subtle and especially dangerous form of gender-based violence in which victims are exploited by their perpetrators using digital means to harass, intimidate, and stalk (Bansal et al., 2023). This frequently involves the sharing of personal data, sexual abuse depicted through pictures, and threats, which are disproportionately predominant to women and marginalized groups (Dunn, 2020). The trends in the legislation approaches to the problem of cyberstalking in India show a considerable shift toward the system that was based on the general provisions of the criminal law and the enactment of highly specific and modern digital statutes which are aimed at punishing the perpetrators to the letter and ensuring the safety of the victims.Legislative Trends in India was fighting cyberstalking with the help of a mix of Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), and Bharatiya Nyaya Sanhita, 2023 (BNS) .

The IT Act, 2000: The government adopted various provisions to deal with the various aspects of online harassment. Section 67 and 67A are examples of sending or publishing salacious and sexually explicit material, which is criminalized. Section 43 and 43A address data damage and hacking frequently employed by stalkers when blackmailing the victims, whereas Section 70 addresses the issue of unauthorized access to the systems.

IPC Provisions: Section 354A, 354D was specially created to deal with the undesired electronic communication, and it is now the rule that continuous, unwanted attempts by a man to communicate to a woman online would qualify as cyberstalking. Others that were used were Section 503 of threatening emails, Section 499 of defamatory messages and Section 420 of online fraud and fake IDs.

The New Criminal Laws (2024): In a major legislative shift, India replaced its colonial-era penal codes with new laws effective July 2024, significantly modernizing the approach to digital crimes. The new cyberspace legislation, specifically the Bharatiya Nyaya Sanhita (BNS) that

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1624-1628

substitutes the IPC, is specifically aimed at cyberstalking in Section 78, and it gives explicit legal provisions on the harsh psychological harm caused by online stalking. In addition, now, under Section 111 of the BNS, cybercrimes are considered as an act of organized crime, and thus, law enforcement may impose much more severe punishment on a person or a group of people who violates digital crimes. The section 78 of BNS adds certain provisions to criminalize kinds of technology supported violence, but the success of this relies on the consistency of interpretation and strict application to the judicial system.

Section 78 of the Bharatiya Nyaya Sanhita, 2023 (BNS) is concerned with the crime of stalking, even that committed using electronic or digital method. The provision makes it illegal to repeatedly follow, contact, monitor or even make an attempt to contact a woman even when she shows a clear lack of interest. Notably, the section specifically acknowledges online stalking, social media monitoring, and tracking over the internet as a constructive stalking, which thus put cyberstalking in the domain of substantive criminal law. The first conviction can only be given a prison sentence of up to three years, in addition to the fine, in accordance with Section 78 BNS, with the punishment being increased on the following conviction. There are also a few exceptions that the provision acknowledges including those committed in order to prevent or detect crime or with legal authority in the event that such acts make sense and are justified. The offence of stalking is criminalised in section 78 of the Bharatiya Nyaya Sanhita, 2023 (BNS), and physical and digital harassment of women are considered. The clause is due to the rising apprehension with regard to incessant and undesired encroachment into the personal space and confidentiality of a woman, even the behaviour conducted via electronics. The section defines stalking as behaviour of any man who makes repeated follow-ups of a woman, contact her, or tries to contact her with a view to creating personal contact or communication with the woman but the woman has indicated that she is not interested. The key aspects of the crime are: (1) a series of actions of following or contacting the woman, (2) desire to have a personal contact, and (3) clear demonstration of disinterest by the woman. The fact that the conduct is persistent even after such refusal is the fundamental pillar of a criminal liability. Notably, it is also applicable in the offence to the digital world. It makes a crime of spying on the internet use or e-mail or any other electronic communication of a woman thus acknowledging cyberstalking as a stalking type. This indicates the nature of the evolving face of harassment in the digital era where surveillance and unwanted communications are in most cases carried out via social media, messaging app, and other internet platforms. Section 78 has exceptions to the crime of stalking specified in the second part (proviso). Although the central clause criminalises persistent following, contacting, or monitoring the digital activity of a woman, the proviso identifies that some of the acts will not in the context of stalking provided that it is legally reasonable, or lawfully approved. Notably, the burden of the accused is on the accused, and the accused has to prove that his actions fall under one of the set exceptions.

1. Crime Preventing or Detection: The former exception can be seen in cases where the act was performed in the role of crime prevention or detection and the accused had been delegated such a position by the State. This clause safeguards the conduct of law enforcement officers, i.e. police officers, investigators or even authorised surveillance officers who can monitor or track a suspect during investigation. The reasoning is that the legitimate state activities should not be criminalised in case performed within the frame of the official responsibilities.

2. Conduct Sought by any Law: The second exception includes the acts carried out under the mandate of any law or to adhere to the legal mandate. As an example, surveillance or contact can be under the order of court, a probation, under the protection, or some other mandate of the law. When this happens, the behavior is said to be legally approved and thus it can not be viewed as stalking.

3. Reasonable and justifiable behavior: The third is a broader one, and it gives the court a chance to evaluate whether the behaviour was also reasonable and justified in the situation. This brings the element of judicial discretion where the courts are able to assess the background, motive, and need of the action. The words are however flexible and as such, courts are called upon to interpret them closely, with a view of ensuring that this defence is not abused. The BNS prescribes the punishment of the offence of stalking in section 78(2) and provides a system of penalties that is graded according to the first-time or repeat offenders. The clause indicates the will of the legislature to discourage the continuity of harassment against women and the need to acknowledge stalking as a way of violation to personal autonomy and privacy. By this provision, any individual found guilty of first time stalking can be sentenced to either a description of imprisonment (either simple or rigorous) up to a term of up to three years, as well as given a fine. The words may extend to suggest that the court can make its own decision on the sentence to be imposed on the convicted individual depending on the facts and circumstances of the case, including the seriousness of the offense, the damage done to the victim, and the motive of the defendant. The provision also brings in the improved punishment on repeat offenders. Should the offender be convicted again or a subsequent time then he or she could be sentenced up to five years imprisonment as well as a fine. This amplification is in accordance with the understanding that the repetition of stalking behaviour shows an ongoing trend of harassment and the neglect of the law hence need to be punished more severely.

SOCIO-LEGAL SIGNIFICANCE

Legally, Section 78 BNS seeks to safeguard the autonomy, dignity, and privacy of women who are the elements of the right to life and personal liberty as stipulated in the Articles 21 of the Constitution of India. Nevertheless, the success of the provision is rather conditional on appropriate enforcement, reporting of the victims, and understanding cyber-related variants of stalking. The proviso attempts to balance two competing interests, where women should not be harassed or victimised by cyberstalking, and lawful or legitimate investigations should not be criminalised. Nonetheless, the open ended character of the reasonable and justified clause can lead to interpretation difficulty that can enable accused individuals to abuse the defence unless it is scrutinized in a stringent manner by the courts. Also, section 78(2) seeks to enhance women protection by deterring recurrent harassment including the effect of cyberstalking as well as indicating to criminology the gravity of such offences. Nevertheless, the success of the provision will be determined at the end of the day by timely reporting, adequate investigation, and judicial sensitiveness in sentencing. Section 78 further gives statutory protection to the autonomy, privacy, and dignity of women in the digital space. When it comes to cyberstalking the success of this provision would heavily rely on the promptness of FIR registration, the preservation of digital evidence, and sensitivity on the part of the police. Therefore, the Section 78 BNS is an avenue that offers an explicit legal framework with the provision bearing a true effect of proper enforcement and centric policing of victims. Other specialized cybercrimes that are discussed by the Bharatiya Nyaya Sanhita, 2023 include sexual harassment, voyeurism and outraging modesty, which provide a wider legal shield against technology-enabled gender-based violence (Foram, 2025). Nonetheless, other legal scholars argue that gender-specific aspects of particular anti-stalking may accidentally exclude male victims or people who consider themselves as gender non-binary and, therefore, introduce the unequal employment of justice (Shambhavee, 2019; Yardley, 2020).

JUDICIAL CONTEXT OF CYBERSTALKING IN THE INDIAN CONTEXT

Indian law has also changed dramatically with the adoption of the Bharatiya Nyaya Sanhita which substitutes the Indian Penal Code and directly criminalizes stalking by way of the Section 78 (Singh, 2025). This new law is expected to overcome the weaknesses of the earlier legal systems, which tended to have a hard time keeping up with the changing forms of cyber-harassment (Shrivastava and Akhter, 2024). Interestingly, the Bharatiya Nyaya Sanhita (Singh, 2025) is an attempt to modernize the Indian legal system through the incorporation of archaic principles with the current legal issues such as new laws on terrorism and organized crime (Meshram, 2024). Although this novel framework is comprehensive, it will be the practice of implementation and application to the judiciary that will define its effectiveness in preventing cyberstalking and giving justice to victims (Manoj et al., 2024). Nonetheless, the above-mentioned sections frequently did not prove to be comprehensive enough in dealing with the multidimensionality of cyberstalking, especially regarding such aspects as image-based sexual abuse and the establishment of fake accounts that are becoming increasingly common in the online world (Halder and Basu, 2024; Paliwal et al., 2024). Instead, the Bharatiya Nyaya Sanhita 2023 proposes more detailed definitions and stiffer punishment on cyber harassment and defamation, as well as on revenge pornography and digital voyeurism, which is a stronger reaction to these ubiquitous problems (Jaishankar, 2016). The Indian judiciary has actively applied these evolving laws to secure convictions and set precedents regarding online harassment. The case analysis of cyberstalking in India shows, the gradual development of recognition of the law and judicial reaction to digital harassment of women is attributed to the development of legal provisions to combat such harassment. Among the first documented cases like **Ritu Kohli case (2000)** which was considered to be the first recorded case of

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1624-1628

cyberstalking in India, it was also brought to light due to misrepresentation of identity by fake online profiles and the lack of special legal provisions to combat such cases; which were then prosecuted in accordance with Section 509 IPC. Much the same case in **State Cyber Cell v. Yogesh Pandurang Prabhu vs. State of Tamil Nadu**. In **Suhas Katti**, the courts have handled the repeated sending of obscene messages, fictitious use of identity and constant harassment and current laws have interpreted the act as cyberstalking and cited mostly the clauses of obscenity and insult to modesty under the IPC and IT act. Other situations, like the one involving **Raju Iyer. Jawaharlal Nehru University**, demonstrate how cyberstalking is achieved through the institutional hierarchies where sexual harassment was through repeated emails and calls, but Mumbai housewife case and the DPS MMS clip case provides a more serious version through pornographic misuse, blackmail and physical effects. In these instances, there are several patterns such as habitual unwanted communication, impersonation, targeting based on gender and devastating psychological and reputational damage on the victims. Simultaneously, the cases reveal serious gaps in the law and procedures, including the lack of special offence of stalking in the prior laws, over-reliance on provisions on obscenity, and lack of the capability to investigate. Through these judicial experiences, stalking, including cyberstalking, as a separate criminal-law offence has eventually been acknowledged, albeit with some difficulty in terms of enforcement, protection of victims, and digital justice.

CHALLENGES IN LAW ENFORCEMENT AND PROSECUTION

Even within the strong legal frameworks, digital evidence collection can pose a major challenge to law enforcement in India as well as the jurisdictional issues that cyberspace presents (Vidani, 2024). What makes matters worse, these difficulties are complicated by the lack of specialized training in dealing with cybercrime cases by policemen, which often results in postponements of the investigation and complicates obtaining a conviction (Kaur et al., 2020). Moreover, police and courts often respond with distrust or victimhood toward victims, forcing them to avoid telling the truth and harming the reputation of the legal system (Padte, 2016). It is also quite difficult to address the cases of cyberstalking as the use of digital technologies is quickly developing, and the legislation and investigation process cannot keep up. It usually leads to a large number of cases being underreported and a perceived impunity of offenders (Borah, 2020; Sati, 2023). This fact shows that the country needs more advanced digital forensics tools and specific cybercrime divisions of the police force that could properly respond to the threat of internet-based stalking that is growing.

CONCLUSION AND RECOMMENDATIONS

The key conclusions regarding the prevalence, consequences, and difficulties of cyberstalking of women in India as an assessment of the effectiveness of the current socio-legal frameworks. The paper tries to offer legislative framework of cyberstalking and challenges in a bid to develop the law enforcement system. The legislative and judicial tendencies towards cyberstalking in India show a very much-needed move to focus on the specifics of the current legal frameworks, instead of using the previously generalized, old-fashioned penal laws and focus on the modern aspect of the matter, yet the practical implementation is also an important challenge. India has shifted the approach of combating cyberstalking by sporadically applying the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC) to the enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS). As explicitly stated in Section 78 of the BNS, digital stalking, such as an internet monitoring and undesirable electronic communications, is directly covered by the scope of criminal law, and substantive statutes have been introduced concerning cyber-stalking. This is a contemporary method that incorporates some form of graded punishment whereby first time offenders are punished not more than three years in jail and repeat offenders not more than five years in jail, where a legislative motive is to ensure that the repetitive harassment is discouraged ruthlessly. In addition, the Indian courts have been at the fore to ensure that digital harassment is legally realized through establishing important precedents. In the landmark cases such as the Ritu Kohli and Suhas Katti case, the general IPC provisions on obscenity and offending modesty had to be used by the courts to convict fake profiles and electronic harassment. Throughout the years as the judiciary has been handling the trends of impersonation, habitual undesired communication, and the devastating psychological effects, they have managed to establish cyberstalking as an independent and serious criminal offense. In spite of the strong token legislative progress, the efficacy of new legislations is largely undermined by structural issues in enforcing the new laws. Jurisdictional challenges, insufficient specialized training in cybercrime, and problems in gathering digital evidence are some of the issues that are often faced by law enforcement. Additionally, a lack of sensitivity in the courts and the police and victim-blaming tend to be the sources of underreporting and delayed justice. Finally, although India has already built a robust and contemporary legal framework to defend the autonomy and privacy of women online, the successful fight against cyberstalking demands an urgent improvement in digital investigation infrastructure, education of law enforcement, and judicial implementation of the new laws with strictness and urgency.

In particular, it will be recommended to cover the gap of the increased awareness of the existing reporting mechanisms, enhance the institutional capacity to manage technology-enabled gender-based violence by training of legal practitioners, and approach the issue of technology-based gender-based violence in a more victim-centrically and gender-just way. The aim of the legislative and policy development should be to close gaps in the existing systems to effectively address the multifaceted nature of the technology-mediated violence and have holistic protection and justice to the victims. The necessity to take into account the establishment of centralized organizations with statutory requirements is also crucial to empower the currently existing mechanisms and ensure a survivor-based approach to overcome technology-imposed violence against women. These should be supplemented with transparent and accessible reporting mechanisms that will bring confidence and make the victims seek justice.

REFERENCES

1. Abdalla, N. M. (2024). Legal Accountability in the Digital Sphere: a Cross-Jurisdictional Study of Social Media Laws in the UK and Bahrain. *Revista de Gestão Social e Ambiental*, *18*(8). https://doi.org/10.24857/rgsa.v18n8-176
2. AllahRakha, N. (2024a). Rethinking Digital Borders to Address Jurisdiction and Governance in the Global Digital Economy. *International Journal of Law and Policy*, *2*(1). https://doi.org/10.59022/ijlp.124
3. AllahRakha, N. (2024b). Transformation of Crimes (Cybercrimes) in Digital Age. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.156
4. AllahRakha, N. (2024c). Global perspectives on cybercrime legislation. *Journal of Infrastructure Policy and Development*, *8*(10), 6007. https://doi.org/10.24294/jipd.v8i10.6007
5. Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating Cases and Digital Evidence. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1). https://doi.org/10.54938/ijemdcsai.2023.02.1.255
6. Bansal, V., Rezwan, M., Iyer, M., Leasure, E., Roth, C., Pal, P., & Hinson, L. (2023). A Scoping Review of Technology-Facilitated Gender-Based Violence in Low- and Middle-Income Countries Across Asia [Review of *A Scoping Review of Technology-Facilitated Gender-Based Violence in Low- and Middle-Income Countries Across Asia*]. *Trauma Violence & Abuse*, *25*(1), 463. SAGE Publishing. https://doi.org/10.1177/15248380231154614
7. Basit, L., Santoso, P., & Rizky, F. (2025). Multi-platform analysis of sexual harassment networks: gender dynamics and digital amplification. *Social Network Analysis and Mining*, *16*(1). https://doi.org/10.1007/s13278-025-01563-3
8. Bezzina, M., Sammut, F., & Scerri, J. (2025). Surrounded by Predators: The Lived Experiences of Online Harassment by Male Public Figures. *International Journal of Bullying Prevention*. https://doi.org/10.1007/s42380-025-00325-1
9. Borah, U. (2020). Cyber Crime against Women in the Digital ERA: A Breif Indian Scenerio. *International Journal for Research in Applied Science and Engineering Technology*, *8*(7), 615. https://doi.org/10.22214/ijraset.2020.30295
10. Burrow, J. G., Kelly, H. D., & Francis, B. E. (2020). Forensic and Legal Medicine. In *Elsevier eBooks* (p. 590). Elsevier BV. https://doi.org/10.1016/b978-0-7020-6223-0.00024-8
11. DEEPAK. (2025). CYBERCRIME VICTIMIZATION OF WOMEN: A CRITICAL STUDY. *Indian Journal of Legal Review*, *5*(14), 1020. https://doi.org/10.65393/zdvh8370

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1624-1628

12. Deo, N., & Singh, P. A. (2022). *Cybersecurity and Sustainable Development* (p. 188). https://doi.org/10.55662/book.2022ccrs.009
13. Dunn, S. (2020). Technology-facilitated gender-based violence: an overview. *SSRN Electronic Journal*. https://apo.org.au/sites/default/files/resource-files/2020-12/apo-nid309987.pdf
14. *Experiencing technology-facilitated gender-based violence in India*. (2025). https://doi.org/10.64185/pppp0127
15. Fernández-Cruz, V., Agustina, J. R., & Ngo, F. T. (2021). An Exploratory Investigation of Traditional Stalking and Cyberstalking Victimization among University Students in Spain and the United States: A Comparative Analysis. *IDP Revista de Internet Derecho y Política*, *32*. https://doi.org/10.7238/idp.v0i32.373814
16. Foram, J. (2025). Cybercrimes and the Legal Framework of India. *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.5281/zenodo.17588657
17. Gurumurthy, A., Vasudevan, A., & Chami, N. (2019). Born Digital, Born Free? A Socio-Legal Study on Young Women's Experiences of Online Violence in South India. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3873875
18. Halder, D. (2015). Cyber stalking victimisation of women: Evaluating the effectiveness of current laws in India from restorative justice and therapeutic jurisprudential perspectives. *Temida*, *18*(3–4), 103–130. https://doi.org/10.2298/tem1504103h
19. Halder, D., & Basu, S. (2024). Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India. *Information & Communications Technology Law*, *34*(2), 163. https://doi.org/10.1080/13600834.2024.2408914
20. Harshit, H. (2025). Legal Framework Against Cyber Bullying In India: A Comparative Study With Usa. *International Journal of Research Publication and Reviews*, *6*(11), 5038. https://doi.org/10.55248/gengpi.06.1125.38172
21. Hedidi, M. (2023). Perspective Chapter: Sexual Cybercrime – The Transition from the Virtual Aggression to the Physical Aggression. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.108786
22. Holt, T. J., Lee, J. R., Liggett, R., Holt, K., & Bossler, A. M. (2019). Examining Perceptions of Online Harassment among Constables in England and Wales. *International Journal of Cybersecurity Intelligence and Cybercrime*, *2*(1), 24. https://doi.org/10.52306/02010319lfqz1592
23. Jaishankar, K. (2016). *Cyber Crimes Against Women in India*. https://openlibrary.org/books/OL28613108M/Cyber_Crimes_Against_Women_in_India
24. Kamarudin, A., Kamarudin, I., & Sanek, S. K. A. (2025). BRIDGING THE GAPS IN MALAYSIA'S CYBERBULLYING LAWS: CHALLENGES AND REFORM PROPOSALS. *International Journal of Law Government and Communication*, *10*(39), 133. https://doi.org/10.35631/ijlgc.1039008
25. Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2020). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, *163*, 120426. https://doi.org/10.1016/j.techfore.2020.120426
26. Kavathekar, A. B. & ILS Law College, Pune. (2021). CYBER CRIME AGAINST WOMEN: ISSUE OF VIOLATION OF RIGHT TO PRIVACY AND RIGHT OF DIGNITY. In *NAVJYOT: Vol. XIII* (Issue IV, p. 48) [Journal-article]. https://navjyot.net/wp-content/uploads/2025/03/9.pdf
27. Laffier, J., & Rehman, A. (2023). Deepfakes and Harm to Women. *Journal of Digital Life and Learning*, *3*(1), 1. https://doi.org/10.51357/jdll.v3i1.218
28. Lal, D. M., Giri, U. K., & Tiwari, S. K. (2024). Virtual Vulnerability: Addressing Cyber Harassment against Women in India. *DS Journal of Cyber Security*, 1. https://doi.org/10.59232/cys-v2i3p101
29. Lazarus, S. (2019). Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. *International Social Science Journal*, *69*(231), 15. https://doi.org/10.1111/issj.12201
30. Manjunath, M., & S, D. S. (2024). A Study on Cyber Frauds Post Digitalization in India. *International Journal for Research in Applied Science and Engineering Technology*, *12*(4), 1790. https://doi.org/10.22214/ijraset.2024.60191
31. Manoj, D., James, R. I., Kumaran, S., Devnath, G. P., Varughese, B. T., Arakkal, A. L., & Johnson, L. R. (2024). Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation. *Child Protection and Practice*, *4*, 100088. https://doi.org/10.1016/j.chipro.2024.100088
32. Marganski, A., & Melander, L. A. (2021). Technology-Facilitated Violence Against Women and Girls in Public and Private Spheres: Moving from Enemy to Ally. In *Emerald Publishing Limited eBooks* (p. 623). https://doi.org/10.1108/978-1-83982-848-520211046
33. McGlynn, C. (2024). Towards a New Criminal Offence of Intimate Intrusions. *Feminist Legal Studies*, *32*(2), 189. https://doi.org/10.1007/s10691-024-09547-y
34. Meshram, B. B. (2024). *Strengthening Digital Justice Governance: A Decision Science Approach to Amendments in ITA 2000, BNS 2023, And BSA 2023 For Next-Generation Cybercrime*. 11151. https://doi.org/10.53555/kuey.v30i4.9720
35. Millar, K., Shires, J., & Tropina, T. (2021). *Gender Approaches to Cybersecurity: Design, Defence and Response*. https://doi.org/10.37559/gen/21/01
36. Miller, L. (2012). Stalking: Patterns, motives, and intervention strategies. *Aggression and Violent Behavior*, *17*(6), 495. https://doi.org/10.1016/j.avb.2012.07.001
37. Mythili, K., & Nagamani, K. (2025). Safeguarding women in digital spaces: Legal responses to cyber harassment and objectification on social media. *Development Policy Review*, *43*(5). https://doi.org/10.1111/dpr.70039
38. Ogilvie, E. (2000). Cyberstalking: Trends and issues in crime and criminal justice. *Australian Institute of Criminology*, 166. https://www.aic.gov.au/sites/default/files/2020-05/tandi166.pdf
39. Padte, R. K. (2016). ¿Están las mujeres seguras? Género, hostigamiento online y ley en India. *Revista Chilena de Derecho y Tecnología*, *5*(1). https://doi.org/10.5354/0719-2584.2016.41269
40. Paliwal, M. G. (2024). *Unveiling the Cyber Landscape: Analysis of Cybercrimes Against Women in India and Future Directions*. https://doi.org/10.52783/eel.v14i2.1468
41. Panda, S. (2023). Towards a Cyberfeminist Framework for Addressing Gender-Based Violence in Social Media. In *Advances in human and social aspects of technology book series* (p. 108). IGI Global. https://doi.org/10.4018/978-1-6684-8893-5.ch008
42. Payne-James, J., & Byard, R. W. (2023). Forensic and Legal Medicine. In *CRC Press eBooks*. Informa. https://doi.org/10.1201/9781003138754
43. Rakha, N. A. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, 23. https://doi.org/10.22201/iij.24485306e.2024.2.18892
44. Rigotti, C. (2024). International Law, Technology, and Gender-Based Violence. In *Oxford Research Encyclopedia of International Studies*. https://doi.org/10.1093/acrefore/9780190846626.013.822
45. Sati, M. (2023). Cyber Crimes and Harassment of Women: An Analysis of the Legal Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4546470
46. Shah, J. (2016). A Study of Awareness About Cyber Laws for Indian Youth. *International Journal of Trend in Scientific Research and Development*. https://doi.org/10.31142/ijtsrd54
47. Shambhavee, H. M. (2019). Cyber-Stalking: Threat to People or Bane to Technology. *International Journal of Trend in Scientific Research and Development*, 350. https://doi.org/10.31142/ijtsrd21354
48. Shrivastava, H., & Akhter, S. (2024). A Comparative Study of the Indian Penal Code and the Bharatiya Nyaya Sanhita's Gender-related Provisions. *Statute Law Review*, *45*(2). https://doi.org/10.1093/slr/hmae033
49. Singh, A. K. (2025). Stalking under the Bharatiya Nyaya Sanhita (BNS): meaning, precautions, enforcement and the apprehensions about misuse. *Indian Journal of Law.*, *3*(5), 13. https://doi.org/10.36676/ijl.v3.i5.119
50. Singh, P. (2018). Cyber crime against women in India [Information and Library Network]. In *Shodhganga*. https://shodhganga.inflibnet.ac.in/handle/10603/267019
51. Singh, V., & Gautam, D. R. (2022). *Cyber Crime, Security and Regulation in India* (p. 147). https://doi.org/10.55662/book.2022ccrs.005
52. Udai, N., & Sharma, D. (2025). Navigating the Digital Landscape: A Study on Cyber Safety and Digital Harassment in College Campus Among Female Students. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5231387
53. Vidani, J. (2024). Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4849742
54. Yardley, E. (2020). Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework. *Violence Against Women*, *27*(10), 1479. https://doi.org/10.1177/1077801220947172.