International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 16-01-2026, Accepted: 17-02-2026, Published: 03-03-2026
Volume 12, Issue 1, 2026, Page No. 383-392

Reconceptualising cyberstalking regulation in India: From a disjointed legal framework to proactive digital safety governance

Madhumitha Gopinath
Advocate, Bar Council of Tamil Nadu and Puducherry, Tamil Nadu, India

Abstract
Cyberstalking is one of the most complicated forms of technology-enabled violence in the new digital era. Although India has updated its criminal law system by passing the Bharatiya Nyaya Sanhita, 2023 and is still using the Information Technology Act, 2000 to address cyber-related crimes, the framework of dealing with cyberstalking is still poorly developed and inadequately organized. The paper provides a critical examination of the current Indian legal framework which deals with cyberstalking, and also points out structural gaps and also assesses enforcement and jurisdictional obstacles. It further explores other jurisdictional comparative developments in order to point out some of the preventive and victim-centred measures like digital protection orders and expedited content removal tools. The paper makes the case in favor of a radical, gender-neutral with technological adaptability legislative change. The paper concludes that India needs to shift towards reactive criminalisation to proactive regulation of digital safety, so that it could adequately respond to the new types of technology facilitated abuse.

Keywords: Cyberstalking, bharatiya nyaya sanhita, 2023, digital safety reform, jurisdictional challenges in cyberspace, victim-centred legal framework

Introduction

With the rapid digitisation, especially after the pandemic has triggered the growth of online interaction, physical stalking has moved to virtual stalking. Due to the development of the social network, messengers, spyware, and tracker technologies, tracking and harassing people has never been as easy and anonymous as it is now. The internet has created the impact of instant communication and easy exchange of data, people can interact and get information with a single click. Nevertheless, the connectivity has also brought out structural weaknesses that criminals take advantage of leading to a continued increase in cybercrime in India. Online stalking or internet stalking, which is also known as cyberstalking, is one such emerging cyber offence. It entails to a wide extent, harassing, intimidating or spying on someone using technology especially using the internet. Surveillance on the Internet, causing threats, identity theft, abuse of personal information, morphing, and constant undesired contact are typical examples of this crime. Cyberstalking is frequently described as an obsessive and illegal surveillance of another human being online presence, which does not require physical interaction but has a significant psychological and reputational damage.

The high rate of digitisation of Indian society, as a result of remote work, online education, internet based payment, and more active social media use, has led to an erosion of the boundary between the personal and the public. People are often posting personal photos, location information and day to day activities on the internet, and they do not have sufficient knowledge regarding digital dangers. This exposure opens certain ways to misuse it, as the personal information may be used by the perpetrators to intimidate, blackmail, or damage their image. In comparison to normal stalking, cyberstalking does not consider geographical boundaries, as offenders can work anonymously and in different jurisdictions which makes them hard to investigate and prosecute.

The recent legislation of the Bharatiya Nyaya Sanhita, 2023 [22] is one of the essential changes in the criminal law system in India. Having killed the Indian Penal Code, 1860, crimes concerning stalking and online harassment are now to be analyzed under the new statutory framework along with the Information Technology Act, 2000 [21]. Although stalking remains to be considered as a punishable offense, the changing digital environment demands more explicit legal definitions, drafting that is technologically sensitive, and easier victim-focused protective measures. The adoption of the new criminal codes gives a significant occasion to reevaluate the idea whether the Indian legal system is sufficient to respond to the challenges of cyberstalking. Cyberstalking is also to be perceived as a constitutional matter.

The Supreme Court, in the case of Justice K.S. Puttaswamy v. UOI has identified the right to privacy, dignity and informational self-determination as one of the fundamental rights under the Article 21. Constant supervision in cyberspace, abuse of personal information, and digital bullying have direct negative effects on the freedom and mental health of a person. In such a way, cyberstalking is not only a violation of the law but also a usurpation of the field of personal freedom ensured by the Constitution. The need to reform is further encouraged by empirical trends.

According to the report released by the National Crime Records Bureau, the crime rate as far as cybercrime is concerned has been increasing dramatically over the last few years. Even though cyberstalking falls under larger and more broadly defined phenomena, including online harassment and sexual exploitation, its effects are frequently powerful and long-term in nature, which impacts not only the mental health of the victims but also their employment and social status. The increasingly statistical trend

demonstrates that there is a necessity to have a legal framework that is cross jurisdictional, gender neutral, and technologically adaptive, which can help overcome cross border and jurisdictional issues. Similar trends in other jurisdictions (United Kingdom, United States, or Singapore) have shown the implementation of specialised digital protection strategies, such as restraining orders, expedited content removal processes, and increased accountability of a platform. Conversely, India still has to depend mainly on the general criminal law and few cyber-specific laws. This imbalance makes the current policy of India and the establishment of a more proactive and prophylactic regime of digital safety a question to be evaluated critically.

Research Objectives

1. To examine the concept, nature, and constitutional aspects of cyberstalking in India, especially regarding privacy, dignity, and digital autonomy.
2. To critically analyse the current laws that regulate the issue of cyberstalking in India such as the Indian Penal Code, 1860 and the Information Technology Act, 2000 [21] and outline the shortcomings of the laws.
3. To evaluate judicial interpretations and the efficiency of lawful solutions to cyberstalking in India.
4. To undertake a comparative analysis of legislations regarding cyberstalking in India and some foreign countries (including the United Kingdom, United States, and Singapore) and suggest the required changes in legislation in India.

Research Questions

1. Does the existing Indian legal framework sufficient to handle cyberstalking in light of constitutional provisions of privacy and dignity?
2. How have Indian courts made of statutory provisions against cyberstalking and what difficulties have remained in enforcing the statutory provisions?
3. Which lessons can India learn based on experience in other jurisdictions to create a more inclusive, gender-neutral, and victim-focused legal system to address cyberstalking?

Hypothesis

The current legal framework as it is represented by the Bharatiya Nyaya Sanhita, 2023 [22] and the Information technology act, 2000 [21] is inadequate in the structure of dealing with cyberstalking because of the lack of clarity in its definitions, the absence of preventive measures through the application of digital restraining orders, and enforcement barriers caused by jurisdictional and cross-border issues, which need to be resolved through comprehensive legislative reform.

Review of Literature

Pritam Banerjee & Dr. Pradip Banerjee, Analysing The Crime Of Cyberstalking As A Threat For Privacy Right In India, Ijlr (2022) [6]

This article analyse the Crime of Cyberstalking as a Threat for Privacy Right in India, consider the subject matter in question. The authors examine cyberstalking as a new menace to the right to privacy and examine the legal provisions in international jurisdictions. They question the Indian system of laws and recommend the study of the advanced countries to develop the country law. The analysis is however not based on the application of the Bharatiya Nyaya Sanhita, 2023 [22], and as such, it cannot be used to assess the ramifications of the new criminal law regime.

Shivangi, Cyberstalking and Its Impact on Vulnerable Group: Women And Minors, LSI (2020) [5]

In this article, Cyberstalking and Its Impact on Vulnerable Group: Women and Minors (LSI, 2020) [5], Author speaks on numerous aspects of cyberstalking, such as the types of stalkers and the laws that act as a response to it as per the Information Technology Act, 2000 [21], and the Indian Penal Code that existed back in 1860. The author points out the disproportionate effect of women and minors and notes an increase in the COVID-19 pandemic. The research is a contribution to the role of victim vulnerability, but is generally descriptive in nature and fails to critically review the gaps in enforcement across the world or international benchmarks.

Dr.Hema Menon, Cyber Stalking In the Indian Scenario and the Indian Information Technology Act, 2008 [7], AAIRJS (2020)

In the article, Cyber Stalking in the Indian Scenario and the Indian Information Technology Act of 2008 [7] (AAIRJS, 2020), author investigates the elements of cyberstalking as a criminal offense in the Indian legal system and discusses both reported and unreported cases. This research paper seeks to lead attention towards information technology act of cyberstalking in terms of legislation. Nevertheless, it fails to fully consider constitutional aspects of privacy and informational autonomy, and it has not made an effort to interact with criminal law changes introduced after 2023.

Jai Shankar Karupannan, Cyber Crime and the Victimization of Women: Laws, Rights and Regulations, IJCC (2012)

In this article, author discusses how women are prone to cybercrime and cyberstalking in particular. The paper provides information on the psychological factors of cyber offenders, legal issues, and enforcement problems. Despite its useful information on the subject of gendered victimisation, the paper has a certain temporal scope and fails to consider the technological progress and the latest changes in the legal field.

1. Concept And Meaning Of Cyberstalking

The term Cyberstalking is used to denote ongoing and unwanted utilization of digital communications technology in harassment, threat, monitoring, or intimidation of a person. Cyberstalking is done electronically unlike traditional stalking, which is carried out using social media tools, emails, messaging services, internet forums and other services offered by the internet. It can be targeted at an individual, group, or organisation and can frequently be in the form of slander, defamation, identity theft, online impersonation, or spreading of personal information.

Fundamentally, cyberstalking involves repetitive and obsessive behaviour, which is done using electronic media with a view to exerting control, threats, humiliation or even psychological torment on the target. The crime does not always imply face-to-face communication and in several situations, victims do not even know that they are being stalked or followed online. This invisibility and anonymity greatly aggravate the damage. Typical manifestations are:

Constant spamming or messages. Development of counterfeit social media accounts in the name of victim. Morphed pictures or defamation postings. Sharing of sexual pictures (revenge pornography) Internet impersonation and identity theft. Intrusion into physical and online location and digital actions. Social networking services allow the provision of personal information, including photographs, contacts, and geolocation, which makes people, especially women and minors, more vulnerable.

Psychological and Sociological Motivations

In many cases, cyberstalking is based on complicated psychological and behavioural drives. Narcissism, obsession, jealousy, revenge, power seeking tendencies, sexual deviance, and psychiatric disorders have also been cited as the underlying factors by scholars. Major motivations include: Jealousy- It is frequently observed among the ex-romantic partners. Obsession and Attraction- One-sided emotional attachment to the victim. Erotomania- Delusional illusion of the victim that he/she is in love with the attacker. Revenge and Hate- Achieving one aim is to take revenge on victims to quench anger or revenge. Sexual Harassment- The use of online resources to consume sexual threat. These motivations are imperative in understanding how to frame preventive and rehabilitative approaches as opposed to treating cyberstalking as a mere penalty concern.

Forms of Cyberstalking

Cyberstalking can be generally described as: Email Stalking- Threatening or harassing emails repeated. Internet/Social Media Stalking- Surveillance and bullying via social network websites, blogs or forums. Computer-Based Stalking- This involves access of personal information or monitoring of online activity with the use of spyware, hacking software or malware. As the stalkerware and surveillance software has appeared, the line between digital and physical stalking is becoming even more unclear.

Types of Cyberstalker

Cyberstalkers can be divided into: Obsessional Stalkers- These are people who had personal relationships previously and were seeking reconciliation or revenge. Obsessive Love Stalkers: This is a one sided emotional attachment that is usually followed by psychological instability. Erotomanic Stalkers- These people are false alarms of believing that the victim also loves them. There are legal and psychological responses that must be differentiated concerning each category.

2. Legislative Framework Governing Cyberstalking In India

There is no separate law against cyberstalking that existed in India as of now. Rather, the crime is handled by a set of general criminal rules enshrined in the Bharatiya Nyaya Sanhita, 2023 [22] alongside particular rules in the Information Technology Act, 2000 [21].

Provisions of Information Technology Act, 2000 [21]

The IT Act offers certain solutions in circumstances in which electronic communication has been abused in cyberstalking: Section 66E -Imposes a penalty on the infringement of privacy of capturing or transmitting any image of a private area without the consent of the individual. Section 67 - proscribes the publication or transmission of obscene content electronically. Section 67A - Deals with the sexually explicit content in electronic form. Section 67B- Relates to child sexual abuse contents in electronic form. Section 72- Punishes violation of confidentiality and privacy. Section 43A -Pits civil liabilities on companies when they fail to secure sensitive personal information.

Under these provisions, there are numerous forms of cyberstalking, which are indirectly addressed, especially when any of the following elements are at play: obscenity, invasion of privacy, or misuse of data.

Provisions under the Bharatiya Nyaya Sanhita, 2023 [22]

Since the IPC has been repealed, the offences of stalking subjects are currently regulated in terms of the Bharatiya Nyaya Sanhita, 2023 [22]. The applicable provisions are:

Stalking (Earlier Section 354D IPC) - Makes illegal recurrent efforts to contact or spy on a woman even when there is plain disinterest even via electronic communication.

1. Any man who,
2. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
3. monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking; Provided that such conduct shall not amount to stalking if the man who pursued it proves that, i. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or
4. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

In the particular circumstances such conduct was reasonable and justified.

2. Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

Voyeurism (Earlier Section 354C IPC): Punishment on the capture and dissemination of images of a woman against her will. Section 77 BNS is the offence of voyeurism. It criminalizes viewing and capturing images of a lady doing personal intimacy acts that she does not desire to be observed. The law establishes strict sanctions, involving imprisonment or financial fines, to first-time and recidivists offenders. It also makes it clear that you should not take pictures in closed places like in the bathroom or doing acts that are not commonly practiced in the open because it is not only that but also sharing the pictures without permission is inappropriate.

"Whoever watches or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on

first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years and shall also be liable to fine and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years and shall also be liable to fine."

Criminal Intimidation (Same Section 503 of IPC prior): Ambiguous threats to reputation or safety. Section 351 of the Bharatiya Nyaya Sanhita (BNS), 2023 [22], claims criminal intimidation to be the method of causing fear to the safety or safety of others or their beloved ones by threat, with the aim of making them do something they do not desire to do or preventing them to perform something legal. The threat may either be verbal, written or through actions. Whoever threatens by any means, another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

"Whoever commits the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Whoever commits the offence of criminal intimidation by treating to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or imprisonment for life, or with imprisonment for a term which may extend to seven years, or to impute unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

Whoever commits the offence of criminal intimidation by an anonymous communication, or having taken precaution to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment provided for the offence under sub-section (1).

Defamation (Earlier Section 499 IPC): Section 356 of BNS Covers reputational damage of online publication. Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes in any manner, any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person."

Observational Analysis

Although these provisions are available, there are still some structural gaps:

Cyberstalking has no separate definition as a digital specific crime.

Gender Specific Drafting: Stalking laws concern mostly women as victims, which restricts the gender-neutrality.

Cross Border Problems: Digital crimes are frequently committed by individuals who are not in India, which makes it difficult to prosecute and extradite them.

Accountability on a Platform: There are few statutory duties placed on social media intermediaries on other than due diligence standards.

Some jurisdictions including the United Kingdom have created the Protection of Harassment Act of 1997 [23] that has incorporated certain stalking offences and restraining orders that apply in regard to online behaviour. In a similar fashion, a number of states in the United States have already passed cyberstalking-specific laws and offer digital harassment specific protection orders. The way India is approaching the issue is still decentralized and reactive, as opposed to proactive as in these jurisdictions. Although there are a set of penal and cyber specific laws that may be used in India to resolve some of the issues of cyberstalking, the fact that there is no such a statutory tool that is both technologically adaptable and victim centric is a challenge to the enforcement. A shift to the Bharatiya Nyaya Sanhita, 2023 [22] offers the chance to update and standardise cyberstalking laws according to the international best practices.

3. Judicial Pronouncement On Cyber Stalking

In India, the jurisprudence of cyberstalking is still developing. Although some of the incidences have been reported in the media, few cases have led to elaborate pronouncements in courts. The judicial line is an embodiment of progressive and ongoing insensitivity, enforcement, and digitalization.

Early Incident- Manish Kathuria Case (Not a Reported Judgment)

Manish Kathuria case (which is considered to be the first cyberstalking case in India) consisted in harassing Ritu Kohli with the use of abusive messages and impersonation on an internet chat room. The misdemeanor claims that the accused posted her phone number online and had to receive numerous obscene calls. This was however not a legal ruling but an early cybercrime complaint that was being addressed by the Delhi Police in the Section 509 of the IPC (since at that time, the Information Technology Act was not yet operational invoked). The case is also historically important since it revealed legislative deficiency and contributed to subsequent modifications of the IT Act, especially the addition of Section 66A (which was ruled unconstitutional). Therefore, it is important in the sense of policy but it is not a binding jurisprudential precedent.

Landmark Judgements

1. Shreya Singhal v. Union of India

This Supreme Court case was not a cyberstalking case but it led to the criminalization of Section 66A of the Information Technology Act, 2000 [21] on the principle of the vagueness and the infringement of the freedom of speech under Article 19(1)(a). The case has an important implication on the prosecution of cyberstalking as: It eliminated a widely broad provision that used to be employed in online harassment cases. It pointed at the necessity of criminal narrowed provisions. It illuminated the constitutional tradeoff between

online abuse protection and freedom of speech. The case changed the prosecutorial environment of cyber crimes in India.

2. State of West Bengal v. Animesh Boxi

In this case, the forgery of false Facebook accounts and the posting of morphed intimate photos of the victim were done. The accused was convicted of the provisions in the IT Act and the IPC (which are now the same under BNS). Understood the great psychological trauma of digital sexual harassment. Considered cyber exploitation as an insult to dignity. Evidence of judicial readiness to punish in online sexual crimes.

3. Kalandi Charan Lenka v. State of Odisha

Here, there was the distribution of obscene messages and morphed pictures of the victim on the Internet. The Orissa High Court acknowledged that the consistent harassment of a person emotionally through the Internet might be regarded as the crimes such as stalking and outraging modesty. The case is important in that, the Court took into consideration the psychological aspect of cyber harassment. It identified digital behavior to be under the old penal regulations.

Judicial Sensitivity Problems.

This has occurred in some bail proceedings like the one of Karan Girotra v. In the case of State (Delhi High Court - anticipatory bail matter), the courts raised some controversial remarks on the behavior of the victim, the delay in reporting the FIR, and consent. These statements indicate that the judicial reluctance to fully realize the digital pressure, abuse, and reputation risks that characterize cyberstalking remains.

Case of Institutional Failure

Vinupriya Case (Policy Failure, Not Precedent)- The Tamil Nadu Vinupriya scandal was a case where some morphed images were circulated resulting in the suicide of the victim. Not a landmark reported judgment, the case pointed to Investigative inefficiency, Police indifference charges, Digital humiliation, Psychological trauma. This case is about systemic failure of enforcement and not judicial logic.

Harassment of Public Figure- Sharmistha Mukherjee Case

Cyberstalking of Sharmistha Mukherjee through sexually explicit Facebook messages has shown that cyberstalking does not discriminate people based on their social or political status. Though the case did not lead to a significant reported judgment, it still highlighted the significance of digital responsibility and swift reaction of the police.

Observation on Indian Judicial Approach

Rather than having a separate cyberstalking law, the courts have used conventional laws such as stalking, intimidation, voyeurism, and defamation to encompass the online activities. Under Article 21, it appears that the constitutional balance between free speech and dignity and privacy tends to be judicial reasoning. There are bail set orders and observations made at the lower court that are indicative of traditional perceptions of victim behavior, lateness of FIR, or consent and require gender-sensitive interpretation. The Indian courts do not have a well -organized system of digital restraining orders (which other countries have). All in all, Indian jurisprudence is developing yet still pervious and reactive as opposed to preventative.

The foreign judicial approach to cyberstalking

The foreign legal systems have crafted more explicit statutory systems and more effective victim protective tools.

United Kingdom: R v. Debnath

Repeated online harassment of the victim was a serious criminal act and conviction was upheld by the Court on digital stalking conduct as provided under the Protection from Harassment Act, 1997 [23].

United States: United States v. Elonis

Another case that the U.S. Supreme Court explained the existence of a criminal intent in cases of online threats is that negligence is not adequate.

People v. Bollaert

The Court affirmed conviction against the operator of the website who had published non-consensual intimate images, acknowledging that the damage to digital reputation was serious.

Foreign Judicial Approach Observation

Some countries such as the UK have clear anti-stalking laws, which are used in case of internet behaviour. The court may grant so called protective or restraining orders that are specific to digital harassment. More emphasis is put on the cooperation of intermediaries and removal of the content. Courts in the U.S. in particular make it clear what the intent requirements are to online threats. Foreign systems focus on short-term relief systems and retribution.

Observations

The foreign jurisprudence is more technologically receptive and shows a more organized system of law than the India. Although the courts in India are increasingly accepting cyberstalking as an offence against dignity and privacy, the application of the law will majorly be based on the adaptation of the old law to the online actions. On the contrary, the foreign jurisdictions have more transparent statutory frameworks and preventive remedies, digital restraining orders, and better institutionalized approaches. The transition to the Bharatiya Nyaya Sanhita, 2023 [22] of India offers continuity, but does not yet add any special purpose cyberstalking law like those found in the UK or the US. Cyberstalking is becoming increasingly visible in India through judicial pronouncements of the increasing recognition of cyberstalking as a grave intrusion into privacy, dignity and personal autonomy. Nevertheless, the lack of a specific legislation leads to the disjointed prosecution in accordance with general criminal laws. The foreign jurisprudence provides some important lessons in the aspects of preventative orders, statutory clarity, and platform responsibility. To adequately solve the issue of cyberstalking in the digital era, Judicial sensitivity should be supplemented by the legislative innovation and institutional reinforcement of India.

4. Comparative Study Of Law Regarding Cyberstalking In Uk And India

The legislation of cyberstalking in India and the United Kingdom is a demonstration of two different philosophies of

legislation. Although neither jurisdiction has passed a law specifically referred to as a Cyberstalking Act, the United Kingdom has evolved a relatively systematic and preventive approach, where India still deals with cyberstalking by an amalgamation of general criminal law and information technology law.

UK

Cyberstalking is dealt with mostly in the United Kingdom through the Protection from Harassment Act 1997 [23], Malicious Communications Act 1988 and Communications Act 2003 [24, 25]. This is due to the fact that stalking is expressly considered to be a criminal offence by the Protection from Harassment Act, especially following its amendment in 2012. Section 2A defines stalking as a summary offence where there must be a course of conduct which constitutes harassment and is considered stalking. The Act gives some examples like stalking an individual, calling or trying to call an individual, publishing about him, surveillance of the internet or electronic communication use, surveillance, spying, and destruction of the property. Notably, the examples listed are not exhaustive meaning that interpretation of the provision can be given such extensiveness to allow courts to respond to changing digital behaviours. Section 4A also makes aggravated stalking, where the acts involve terror of violence or grave alarm or distress which elicits a significant impact on the daily undertakings of the victim, a criminal offense. Besides imprisonment, the courts have the authority of making restraining orders in accordance with the Section 5, even after the person had been acquitted hence taking a preventive measure to ensure that victims are not harmed to an even greater extent.

India

India governs cyberstalking mostly by the Bharatiya Nyaya Sanhita, 2023 [22] and Information Technology Act, 2000 [21]. In the Bharatiya Nyaya Sanhita, Section 78 makes the act of stalking criminal, such as frequent efforts to get in touch with a woman when she has shown no interest and used electronic communication surveillance. Although the clause acknowledges digital surveillance, it fails to hint at the range of technological surveillance, or even discusses the new types of digital surveillance including doxxing, cyber impersonation, or data-based intimidation. The provision is still drafted on gender specific grounds, which restricts its textual application to women as victims, although there are other provisions of the penal that could be applied in case of a male or non-binary victim. The maximum period of punishment is three years in the first instance and five years in the latter instance. Other clauses within the Information Technology Act deal with obscenity, privacy invasion and breach of confidentiality, but these work rather patchily than on a comprehensive cyberstalking platform.

Observations

Comparative analysis shows that the United Kingdom has a more preventive and victim-oriented model. With the existence of restraining orders, courts can be active and limit further interactions via digital means. In the UK, statutory language specifically mentions the surveillance over the usage of internet and the posting of contents online, thus bringing down the interpretative ambiguity. The Indian system on the other hand is very punitive and reactive in nature and is more about punishing the offence after it has taken place and not about structured measures to ensure that the same does not happen again. Moreover, the lack of a digital restraining order system in India puts the victims in a disadvantaged location because the only way the victims are relieved is by criminal prosecution. The other major difference is the breadth of concept of protection.

In the UK, the law is applicable regardless of the gender and is known as a pattern-based crime that is founded on harassment and distress. Although the Indian law is progressive in the criminalisation of electronic monitoring, it still maintains a gender specific language and lacks the statutory elaboration on the conduct of technology. This leaves a lot of interpretative role to the courts and therefore may result into inconsistency. Besides the UK model, there are other jurisdictions which offer the instructive frameworks. The Protection from Harassment Act 2014 [26] of Singapore establishes expedited protection orders and content ordered by courts, thus incorporating both civil and criminal sanctions.

The US also has such laws as federal and state based cyberstalking laws, which provide the option of protective orders and provide very perpetrators with severe punishment in case of interstate cyber harassment. These jurisdictions prioritize victim safety, fast relief, and intermediate cooperation which can be explained by the fact that digital harm is contagious and may be addressed with a fast legal response.

The international trends in comparative legal developments in other countries can be used as good guidance in enhancing the cyberstalking framework of India. Cyberstalking is regulated in the United States by state and federal laws, which criminalize interstate harassment and threats via the electronic medium. The United States has made great emphasis on proving the criminal intent, and at the same time, the courts have made it a priority to ensure that the victims are safe. Protective orders, electronic monitoring terms and high bail are normally required to avoid repeated harassment. The American system acknowledges that the digital threats can develop very quickly and this is why preventive strategies are incorporated into the criminal justice procedure. The U.S. is an example of how the protection of victims may be utilized in conjunction with the constitutional protection of free speech by means of punitive sanctions and enforceable directive on no-contact.

On the same note, Singapore has been particularly progressive and systematic using the Protection against Harassment Act 2014 [26]. The bill establishes a hybrid civil criminal approach through which a victim can obtain an instant Protection Order and Expedited Protection Orders that will enable them to stop the offender and ensure that they do not continue harassing them. It also gives the courts the ability to instruct the internet removal or correction of information, hence dealing with the digital victimization contagion. It is worth mentioning that Singapore has included certain anti doxxing provisions, as it has acknowledged that the possibility of posting personal information online is a significant threat. This combined model means that the victims do not remain a mere dependant of the lengthy criminal proceedings but get interim quick relief, which is a contemporary view of computer vulnerability.

Based on these foreign examples, India can take into account a number of reforms to update its cyberstalking regulation. An independent and broad cyberstalking law would offer some definitional clarity and not depend on isolated statutes found throughout the general criminal law and the information technology legislation. Reform may also involve ensuring that the stalking provision is made a complete gender neutral provision to guarantee that all victims have equal protection regardless of their gender identity. Introducing digital restraining orders which could be imposed by the court at the initial point of the process would greatly benefit the preventive action. Moreover, legalization of doxxing, online impersonation, and technology based coercion would respond to the new types of digital abuse that are not directly defined in the current laws.

Mechanisms of time bounded content removal especially by judicially guided instructions to the intermediaries would minimise reputational losses experienced by victims over time. Creating specialised cybercrime courts or special judicial benches, which have technological skills, might also enhance uniformity and sensitivity of trial. Lastly, enhancing cross border collaboration, including new extradition agreements and mutual legal assistance treaties, would be beneficial to deal with the international nature of cyberstalking crimes.

Simply, comparative analysis has shown that proper regulation of cyberstalking should not only be criminalised, but rather an entire system incorporating prevention, quick response, technological transparency and victim-focused solutions. India will be able to transition to a more responsive and constitutionally balanced digital safety regime by implementing balanced reforms based on the best practices of other countries.

To sum up, although India has acknowledged cyberstalking in its criminal law system through the Bharatiya Nyaya Sanhita, 2023 [22], its legislative framework is relatively conservative and reactive compared to the United Kingdom and other developed jurisdictions. The lack of clear preventive measures and gender neutral draft, as well as the descriptions of technology, restrict the efficacy of enforcement. A more detailed and technologically flexible system, including restraining orders, expedited takedown measures, and more explicit statutory text, would go a long way in enhancing India in combating cyberstalking within the changing digital environment.

5. Analysis On The Current Position Of Cyber Stalking In India

The current legal system of cyberstalking in India is still disjointed and conceptually immature. Despite the enactment of the Information Technology Act, 2000 [21] to deal with cyber offences and replacement of the colonial criminal code with the Bharatiya Nyaya Sanhita, 2023 [22], there is yet to be a single and exclusive standalone law that addresses cyberstalking in India. Rather, the crime is dealt with by some general stalking and harassment clauses with large interpretative and enforcement gaps.

Within the Bharatiya Nyaya Sanhita, stalking has been made a criminal offence which also involves observing the use of internet, email or other electronic communication by the woman. Although such an acknowledgment of online surveillance is a good idea in theory, the facility is structurally flawed. It still maintains gender specific formulation, whereby only women are victims. Cyberstalking in the modern digital world happens to people regardless of their gender, age, and sexual orientation. The gender limited construct hence does not apply to the essence of digital vulnerability, and does not embody the equality before the law principle. A gender neutral alteration would be more consistent with constitutional provisions and victimology in the present times.

The other major weakness is that there is no clarity on the method of monitoring. The provision fails to provide what digital surveillance, algorithmic tracking, use of spyware, social media tracking or data scraping entails. The silence of the law raises ambiguity in prosecution in an age where people can use facial recognition software and metadata to exploit information. Lack of technological determinism compels courts to rely substantially on interpretation hence resulting into inconsistent application.

In addition, the BNS still maintains the clause of insult to modesty or criminal intimidation, which can be applied to the case of a threatening or abusive Internet message. Nevertheless, these provisions were traditionally offline conceptualised. They are not able to describe the special features of cyber abuse that are anonymity, viral spread, identity morphing, deepfakes, or organized online harassment campaigns. Enforcement agencies hence tend to take traditional provisions to accommodate technologically sophisticated conduct resulting in doctrinal ambiguity.

Cyberstalking is also not specifically defined by Information Technology Act, 2000 [21]. Although some of the clauses that are relevant to identity theft, impersonation, violation of privacy and publication of obscene material can be used, the Act mainly touches on commercial and technical cyber crimes. Cyberstalking has psychological, reputational, and coercive aspects, which are not discussed comprehensively. The punishments that are already provided are also not remunerated to accommodate the long-term mental trauma and reputation loss that the victims endure.

Jurisdiction is one of the most urgent problems in the cases of cyberstalking. The cyberspace has no geographical limits but law enforcement agencies are territorial. In instances where the offender and the victim live in separate states or even nations, it becomes complicated in determining in which court to be used. Despite having the Information Technology Act which gives extraterritorial jurisdiction to computer systems offences which involve computer systems situated in India, there is still a problem of practicability in its enforcement. Extradition processes are tedious, rely on dual criminality conditions and limited by diplomacy. Although the Indian criminal law is applicable to offenses that are committed outside India against Indian computer resources, its prosecution with respect to foreign cooperation is not consistent and unguaranteed.

India is not a signatory to the first global convention treaty on cybercrime, the Budapest Convention on Cybercrime. Although the issue of sovereignty and information sharing is still present, non-participation restricts the exchange of India to enjoy the mechanisms of structured transnational cooperation. As cyberstalking is transnational in nature, particularly via social media which are based in different countries, globalised frameworks are more and more requisite.

Enforcement Sometimes, lack of digital forensic expertise, time delays in requesting data via intermediaries, encryption obstacles, and a minimal level of cross-state coordination of

cyber-cells are challenges encountered by investigative agencies. Delay in the process and interim protection are common to victims. Also, a traditional digital restraining order or an expedited online content removal tool just designed to specifically address stalking is not currently offered under Indian law, as it is in some countries and territories. The lack of quick interim solutions implies that dangerous material can still be spread even during legal processes.

Such gaps need structural redress and not ad hoc redress. One of the alternatives that India may contemplate is the passage of an independent Cyberstalking Prevention and Digital Safety Act. Such laws ought to offer an extensive meaning of cyberstalking, which should encompass doxxing, deepfake threats, impersonation, non-consent surveillance, and continuous electronic spying. The law has to be gender-neutral and victim-focused to acknowledge psychological damage as a material injury.

There should also be the introduction of a digital protection order system, which is the ability of the courts to put immediate no contact and no surveillance orders that can be enforceable across electronic platforms. Court-presided time-based content takedown measures would lessen the long term reputational harm. The standards of intermediary liability must be amended to require immediate collaboration with the law enforcement without the violation of the freedom of expression.

There might be special cybercrime courts or special technological benches that would promote judicial expertise and provide uniform interpretation. Repeat offenders may also have a national cyberstalking registry, which would be focused on privacy and serve as a deterrent tool. Moreover, India is advised to enhance the international collaboration by revising the mutual legal assistance treaties and re-evaluate the involvement in the international cybercrime systems to enhance the effectiveness of extradition.

The other research gap that this study has determined is the lack of mental health considerations in the legal response mechanisms. Cyberstalking has long term psychological effects, such as anxiety disorders, depression, damaged reputation, and withdrawal. Nevertheless, current laws theorise the crime as harassment and less as long term psychological abuse. The statutory acknowledgment of trauma-informed support of victims, counselling requirements, or state-funded rehabilitation systems is minimal. The victim compensation schemes and psychological support should be incorporated in the criminal justice process using a holistic approach.

Conclusively, the current framework acknowledges the existence of cyberstalking but does not cover it directly and sufficiently. The legislation is still disjointed, gender limiting, ambiguous in its technology and procedurally slow. These gaps need to be bridged by switching between reactive criminalisation and proactive digital safety governance. An effective legislative, procedural, and institutional reform program would not just empower the protection of victims, but would also make India a progressive jurist system that can nimbly address the emerging digital harms.

Proposed Bill: Cyberstalking Prevention and Digital Safety Act Institutional Support Framework

Although it would be necessary to introduce a standalone Cyberstalking Prevention and Digital Safety Act that would help to address the lack of clarity in definitions and procedures, this would not be a sufficient measure in the form of legislative reform. To be implemented successfully, institutional capacity building and formalized mechanisms of digital governance are needed. Here, the hybrid format of regulation would be suitable, based on the international models of development assistance, including those advocated by the United States Agency for International Development (USAID) and focus on the empowerment of the rule of law, institutional responsibility, and the transformation of the digital government.

In this type of model, the suggested Cyberstalking Prevention and Digital Safety Act will work with a specialised Digital Safety Authority that acts as an independent regulatory and coordination agency. This power would not take the place of the courts or police, but would ensure that the network of law enforcement agencies, digital intermediaries, mental health services, and victim support systems operate in a coordinated manner. The experience of governance models developed by the USAID in different jurisdictions shows that the legal reform should be supported by the training modules, digital infrastructure assistance, awareness programs, and cross border cooperation frameworks to deliver significant results. Implementing such a model in India would make cyberstalking laws more enforceable.

The Act may include the clauses imposing the systematic collaboration between intermediaries and investigative agencies by establishment of regular response schedules in data maintenance and content takedown. Also, a centralised online help desk can be institutionalised where victims can seek immediate relief including interim digital protection orders awaiting the court. This would reflect the development oriented systems of governance that focus on accessibility, transparency and victim focused delivery of justice.

Moreover, the international cooperation mechanisms could be enhanced with the help of the technical assistance program aimed at the training in digital forensics, building the capacity on cyber-investigation, and evidence sharing procedures across the borders. India may also establish expedited mutual legal assistance avenues to cyberstalking incidents employing the foreign platform or criminals in foreign jurisdictions, unlike depending on the conventional extradition methods. Such approach is indicative of the developmental school of thought that institutional preparedness is equally important as statutory criminalisation.

The second noteworthy aspect of the latter model would be the inclusion of the psychological and rehabilitative services in the system of enforcement. An institutional reform model in the USAID style is usually a combination of legal accountability and community resiliency approaches. The implementation of this in India would amount to institutionalizing obligatory counselling support, digital literacy campaigns, and preventive awareness campaigns in the statutory context. A psychological manipulation crime and reputational damage, cyberstalking requires a multidimensional approach and not a strictly punitive one.

Simply put, the suggested Cyberstalking Prevention and Digital Safety Act cannot exist as a penal law but as a component of a larger digital governance ecosystem. India can overcome the current gaps in the legal and enforcement agencies because, in combination with clear criminal

definitions, preventive digital protection orders, speedy content-removal mechanisms, specialised courts, and institutional capacity-building based on international development models of governance, it is possible to bridge the gaps. This framework would not only shift towards reactive prosecution, but create a digital safety management philosophy to ensure that technological advancement does not surpass legal protection.

Conclusion

Cyberstalking in India is a legally recognised but structurally underdeveloped area of the criminal justice system. Even though the provisions in the Bharatiya Nyaya Sanhita, 2023 [22] take into consideration stalking and includes allusions to electronic monitoring, the process is still gender-specific and not sensitive to modern day digital harm. On the same note, the Information Technology Act, 2000 [21] focuses on identity theft, privacy invasion and electronic publication of harmful information, but fails to conceptualize cyberstalking as an offence with psychological, reputational and coercive aspects. The outcome is a piecemeal structure that greatly relies on interpretative extrapolation instead of legislative precision.

The study has shown that cyberstalking cannot be regarded as an implication of offline bullying but a qualitatively different kind of abuse. The spyware, algorithmic tracing, data scraping, facial recognitions, interpersonal actions of impersonation, deepfakes and synchronized internet harassment campaigns generate long lasting and international harms. However, current systems are not designed in a way that they can accommodate such advanced technological behavior. This in turn forces the courts to apply traditional teachings into digital realities, resulting in inconsistency of the doctrines, and inconsistent application.

The problem is further complicated by juridical complexity. There is no limit to the scope of cyberspace, whereas enforcement systems are at the territorial level. There are provisions on extraterritorial jurisdiction in principle but they are not being put into practice due to delays in extradition, dual criminality, diplomatic negotiations and lack of cross border cooperation. The lack of involvement of India in organized global frameworks of cybercrime also restricts the systematic transnational cooperation. Since cyberstalking by its very definition is borderless, the lack of efficient systems of global collaboration poses a serious threat to the safety of victims.

The issue of enforcement constraints in the domestic structures also is acute. The unavailability of digital forensic capacities, a slow process of accessing the intermediate data, encryption, and a lack of coordination among the cyber cells tend to increase the duration of investigation. More importantly, at this point, Indian law does not include any direct digital protective measures like enforceable no contact electronic orders or expedited processes of removing judicial content specifically to address stalking associated harms. This has thus left the victims with reputational and psychological harm even when proceedings are ongoing.

The other major gap that was realized during this research is the lack of understanding of cyberstalking as a long term psychological abuse. The provisions that exist in law define harassment or intimidation as the main concept of it, and ignore its long term effects on mental health, such as anxiety disorders, depression, social withdrawal, and reputational trauma. Lack of trauma based victim care structures, formal counselling systems, and in built compensation systems have shown a biased penal prism instead of a comprehensive justice prism.

The comparative legal processes reveal that the optimal approach to the regulation of cyberstalking is to combine criminalisation with the preventative and victim oriented solutions. Deterrence and protection are improved by the introduction of digital restraining orders, time-limited content takedown systems, and specialised adjudicatory frameworks. Based on such models, the proposed research suggests the following structural changes, such as the enactment of a separate Cyberstalking Prevention and Digital Safety Act, a gender neutral definition, a statutory definition of doxxing and technology facilitated coercion, implementation of digital protection orders, clarification of intermediary liability, specialised cyber benches, reinforcement of international cooperation frameworks and integration of mental health support into the justice process.

Finally, the regulation of cyberstalking in India needs to change toward the prosecution toward the active governance of the digital sphere. Technological change should not be an expected response of law, but must be anticipated. An integrated system of legislative and institutional reform would not only seal the gaps currently available in the doctrines but also revive constitutional pledges in the digital space, of equality, dignity, privacy, and personal freedom. Through a technologically responsive, victim-oriented, and intergovernmental approach, India can drift to more resilient and progressive cyber justice structure, which can currently respond to emerging digital harms in an increasingly flexible technological environment.

References

1. Sharma S. Regulatory Framework for Combating Cyberstalking and Online Harassment in India. Indian J. Legal Rev, 2025. https://ijlr.iledu.in/regulatory-framework-for-combatting-cyberstalking-and-online-harassment/
2. Citron DK. Cyber Civil Rights. B.U. L. Rev,2009:89:61.
3. Chandra A. Privacy and the Indian Constitution after Puttaswamy. Indian J. Const. L.,2017:9:1.
4. Verma A. The Quest for Justice: Cyberstalking Against Women in India. Lex Localis J. of Local Self-Gov't, 2023. https://lex-localis.org/index.php/LexLocalis/article/
5. Shivangi. Cyberstalking and Its Impact on Vulnerable Groups: Women and Minors. Legal Serv. India, 2020.
6. Banerjee P, Banerjee P. Analysing the Crime of Cyberstalking as a Threat for Privacy Right in India. Academia, 2022.
7. Menon H. Cyber Stalking in the Indian Scenario and the Indian Information Technology Act, 2008. Asian Acad. Res. J. Soc. Sci. & Human, 2020, 7.
8. Bhatia G. The Transformative Constitution and Digital Freedoms. NUJS L. Rev,2019:12:45.
9. McGlynn C, Rackley E. Image-Based Sexual Abuse. Oxford J. Legal Stud,2017:37:534.
10. Brenner SW, Rehberg M. "Kiddie Crime"? The Utility of Criminal Law in Controlling Cyberstalking. First Amend. L. Rev,2009:8:1.
11. Kerr OS. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. N.Y.U. L. Rev,2003:78:1596.

12. Clough J. Principles of Cybercrime Legislation. Crim. L. & Phil.,2016:10:1.
13. Berman PS. The Globalization of Jurisdiction. U. Pa. L. Rev,2002:151:311.
14. Spitzberg BH, Hoobler G. Cyberstalking and the Technologies of Interpersonal Terrorism. New Media & Soc'y,2018:30:1.
15. Rodrigues V. Cyber Stalking: Issues of Enforcement in Cyberspace. IJLMH,2020:3:580.
16. Journal of Interpersonal Violence. https://journals.sagepub.com/home/jiv
17. International Journal of Cyber Criminology. https://www.cybercrimejournal.com/
18. Journal of Cybersecurity. https://academic.oup.com/cybersecurity
19. Violence Against Women. https://journals.sagepub.com/home/vaw
20. U.S. Agency for International Development. Digital Policy (2024–2034), 2024. https://www.usaid.gov/digital-policy
21. Information Technology Act. No. 21 of 2000.
22. Bharatiya Nyaya Sanhita. No. 45 of 2023.
23. Protection from Harassment Act 1997.
24. Malicious Communications Act 1988.
25. Communications Act 2003, c. 21.
26. Protection from Harassment Act 2014.
27. 18 U.S.C. § 2261A.
28. K.S. Puttaswamy v. Union of India,2017:10 SCC 1.
29. Shreya Singhal v. Union of India,2015:5 SCC 1.
30. State of W.B. v. Animesh Boxi,2018 SCC OnLine Cal 180.
31. Kalandi Charan Lenka v. State of Odisha,2017 SCC OnLine Ori 397.
32. Karan Girotra v. State (NCT of Delhi),2023 SCC OnLine Del 2194.
33. R v. Debnath,2005 EWCA Crim 3472.
34. Elonis v. United States,2015:575 U.S. 723.
35. People v. Bollaert,2016:248 Cal. App. 4th 699.
36. National Crime Records Bureau. Crime in India 2022,2023.
37. USAID. Digital Policy (2024–2034), 2024.