Page 1446 – 1466 **DOI:** *https://doij.org/10.10000/IJLMH.1111639*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Cyberstalking in the Digital Age

AKANKSHYA DAS[1] AND SAMBHAB SWAIN[2]

ABSTRACT

The internet and the rapid advancement of digital technologies have altered the way people converse and interact in the modern society. Despite the fact that communication has become easier and quicker through these advancements in technology, it has provided more avenues through which crimes can be committed in cyberspace. One of such emerging issues is cyberstalking, which can be described as a continuous use of electronic channels of communication such as emails, social networks, instant messages, or any other digital channels to harass, intimidate, spy or threaten another individual. Unlike in the conventional stalking, in cyberstalking, no physical proximity is involved and criminals can easily hide their identity behind the anonymity most digital platforms provide, making it much more difficult to detect and prosecute them. In the present digital era, people share personal information, photos, and interaction with daily activities in the cyberspace. This augmented internet presence exposes persons to greater susceptibility of victimisation. Some of the activities that cyber stalkers may engage in are sending threatening messages, creation of fake online profiles, defamation spread, unauthorised use of personal accounts or continuous monitoring of the online activities of a victim. These activities are a grave violation of the privacy of the involved person and often result in psychological distress, fear, emotional trauma, and reputational damage. The Indian courts have largely used the provisions of the Information Technology Act, 2000, and some of the criminal law provisions that deal with stalking and harassment to take legal action against cyberstalking. However, the legal system is still developing, and such problems as jurisdiction, the lack of specific laws against cyberstalking, and the lack of knowledge about the solutions regarding the issue by victims are still a challenge. This paper reviews cyberstalking in this digital era, its impact on victims and society and the sufficiency of the current Indian law. It calls on the need to improve legal processes, increases awareness, and more preventive actions to safeguard individuals in the digital community.

Keywords: *Cyberstalking, Cybercrime, Online Harassment, Digital Privacy, Information Technology Act.*

I. INTRODUCTION

The internet and digital communication technologies have developed rapidly, fundamentally

[1] Author is a Student at KIIT School of Law, Bhubaneswar, Odisha, India.
[2] Author is a Student at KIIT School of Law, Bhubaneswar, Odisha, India.

 [ISSN 2581-5369]

altering how individuals interact and communicate. Social media platforms, email services, messaging applications, and other digital tools have made communication faster and more convenient than ever before. Nevertheless, these technological innovations have also created possibilities for new crimes in cyberspace. Cyberstalking is one of the most pressing emerging issues in the contemporary digital world, defined as the use of electronic communication and internet-based infrastructure to perpetrate repetitive harassment, threats, surveillance, and intimidation upon another person. Unlike traditional stalking, it does not require physical proximity between the perpetrator and the victim.[3]

With the help of digital tools, criminals can easily monitor the activities of a person, send threatening messages, impersonate their profile, or spread false information about them. The anonymity that the internet provides usually allows criminals to conceal their identity, making it hard to trace and convict them. People often post their personal information, photographs, and location on websites and social media. Although these practices improve social interaction, they expose users to cybercrimes such as cyberstalking. Criminals can misuse such information to intimidate, blackmail, or defame victims. Consequently, cyberstalking may lead to severe psychological and emotional harm, including fear, anxiety, depression, and reputation destruction.

In India, the rise in the use of digital platforms has correspondingly increased cases of cybercrimes including cyberstalking. While some legal provisions exist under the Information Technology Act, 2000, and other criminal laws, the legal framework governing cyberstalking continues to evolve. There is accordingly a need to review the concept of cyberstalking and to assess whether the legal frameworks presently in place are adequate to address this growing threat.

II. CONCEPTUAL FRAMEWORK OF CYBERSTALKING

A number of researchers and legal scholars have examined the question of cyberstalking from various fronts. According to much of the existing scholarship, cyberstalking is a category of technology-aided harassment in which perpetrators employ digital communication tools to threaten or harass their victims. Scholars have highlighted that anonymity in cyberspace contributes significantly to such behaviour, since criminals generally believe they cannot be easily tracked. In India, no single dedicated law directly addresses cyberstalking. Rather,

[3] Information Technology Act, 2000, No. 21 of 2000 (India); Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, s. 78 (criminalising stalking including electronic monitoring).

 [ISSN 2581-5369]

different provisions in existing statutes are applied to address such offences.[4]

The Information Technology Act, 2000, contains provisions relevant to identity theft, breach of privacy, and the publication of obscene content in electronic form. Provisions of criminal law addressing stalking, defamation, criminal intimidation, and voyeurism can also be invoked in cases of online harassment. Despite these provisions, legal scholars consistently note that the existing framework is disjointed. Most of these laws were originally designed to address analogous offline crimes and are now being stretched to cover cybercrimes, creating a number of enforcement difficulties, particularly where perpetrators are anonymous or act across multiple jurisdictions.

A. Meaning and Evolution

The notion of cyberstalking, as a unique category of cybercrime, entails the repetitive and sustained use of digital communication media for the purpose of harassing, intimidating, or surveilling an individual. Unlike the conventional notion of stalking, where the primary factor is the physical proximity and direct surveillance, the virtual world of cyberstalking allows the perpetrator to utilize the electronic medium, including social media, email, instant messaging, or other internet-based tools, for the purpose of targeting the victim. The essential characteristic of cyberstalking, however, does not entail the singular incidents of online harassment but the repetitive pattern of behavior, which evokes feelings of intimidation, apprehension, and the sense of virtual surveillance in the minds of the victim.

It has become one of the biggest dilemma of contemporary cyber law due to the high growth in the use of internet and online communication. Now more than ever before, people are sharing personal information on the Internet more often than ever due to the proliferation of smartphones, social media platforms, and instant messaging services. Although this digital environment has improved communication and connectivity, it has also led to new avenues of misuse of technology by cybercriminals to harass and intimidate others. Cyberstalking represents one such misuse of technology, where individuals repeatedly target victims through digital means to threaten, monitor, or psychologically disturb them.[5]

From the legal perspective, the notion of cyberstalking has not been recognized as a distinct category of offense in India or other jurisdictions. Rather, it has been viewed as an aggravated form or variant of conventional offenses such as stalking, harassment, defamation, or criminal

[4] Viola Rodrigues, 'Cyber Stalking: Issues of Enforcement in Cyber Space' (2020) 3(2) International Journal of Law Management & Humanities 568, 570–571.
[5] Udit Agnihotri and Narendra Kumar Thapak, 'The Cyberstalking Situation in India: A Social, Legal, and Technological Viewpoint' (2024) 15 Purva Mimaansa 34, 35.

 [ISSN 2581-5369]

intimidation. The lack of legal recognition for the notion of cyberstalking has, in turn, led to the absence of a universally accepted definition, with the legal world seeking to address the issue through the interplay of statutory provisions and judicial decisions. The recognition of the factor of electronic monitoring in the definition of stalking, as embodied in Section 78 of the Bharatiya Nyaya Sanhita, 2023, however, appears to be an attempt to recognize the notion of cyberstalking.

The development of the concept of cyberstalking can be directly correlated to the development of the digital ecosystem and the increased rate of digitalization in the world. During the early days of internet development, the cyberstalking idea was limited to emails and online chat rooms where the anonymity of the perpetrator assisted them in continuously bombarding the victim with the threats or abuses. However, the development of social media, smartphones, and other such tools has helped the concept of cyberstalking to transform into a multi-dimensional form, where the offender can continuously monitor the activities of the victim through social media posts, stories, geotags, and digital footprints, thus transforming cyberspace into an instrument for continuous intrusion into the life of the victim.

The anonymity factor plays an important part in the development of the concept of cyberstalking. Unlike other conventional crimes, where the identity of the offender can be known or traced, the cyberspace provides the offender the opportunity to remain anonymous through the use of fake accounts, virtual private networks, or other such tools, thus creating challenges for the law enforcement agencies in this regard. Cyberstalking has thus evolved into a borderless crime, where the geographical boundaries cannot be defined, thus creating challenges for the law enforcement agencies in this regard.

Another important factor in the development of the concept of cyberstalking is the transformation from the conventional form of stalking, where the offender only harasses the victim, into the form where the offender, along with several others, engages in the act of dogpiling, where several individuals collectively engage in the act of harassment. The development of new-age technologies such as artificial intelligence tools has also helped the concept of cyberstalking to transform into the form where the offender engages in the act of creating fake images or videos to defame the victim, thus transforming the concept into a new form, where the conventional forms of harassment are not applicable.

In the context of India, the evolution of cyber stalking has been directly related to the rapid increase in internet penetration and social media use. While this has been a positive force from the standpoint of improving communication and accessibility, it has also led to an increase in

 [ISSN 2581-5369]

the vulnerability of individuals to cybercrimes. The widespread use of personal information on the internet has led to an increase in the vulnerability of individuals to stalking, imitation, and harassment, even as cyber stalking has been recognized under various legal provisions.

In a broad sense, cyber stalking may be seen as an interface between technology and criminal intent, wherein stalking is defined from a conventional perspective within the context of the internet and other information technologies. The evolution of cyber stalking has been directly related to the lack of conventional legal frameworks, which have been unable to keep pace with the evolving nature of this crime. [6]

B. Forms and Methods of Cyberstalking

Cyberstalking may occur in several forms depending on the method employed by the offender. One common method is repeated online communication through emails or messages that threaten or harass the victim. Another method involves impersonation, where the offender creates fake social media accounts using the victim's name or personal information to spread defamatory content. In many cases, cyber stalkers also monitor the victim's online activities by tracking their posts, comments, or location updates on social media platforms.[7]

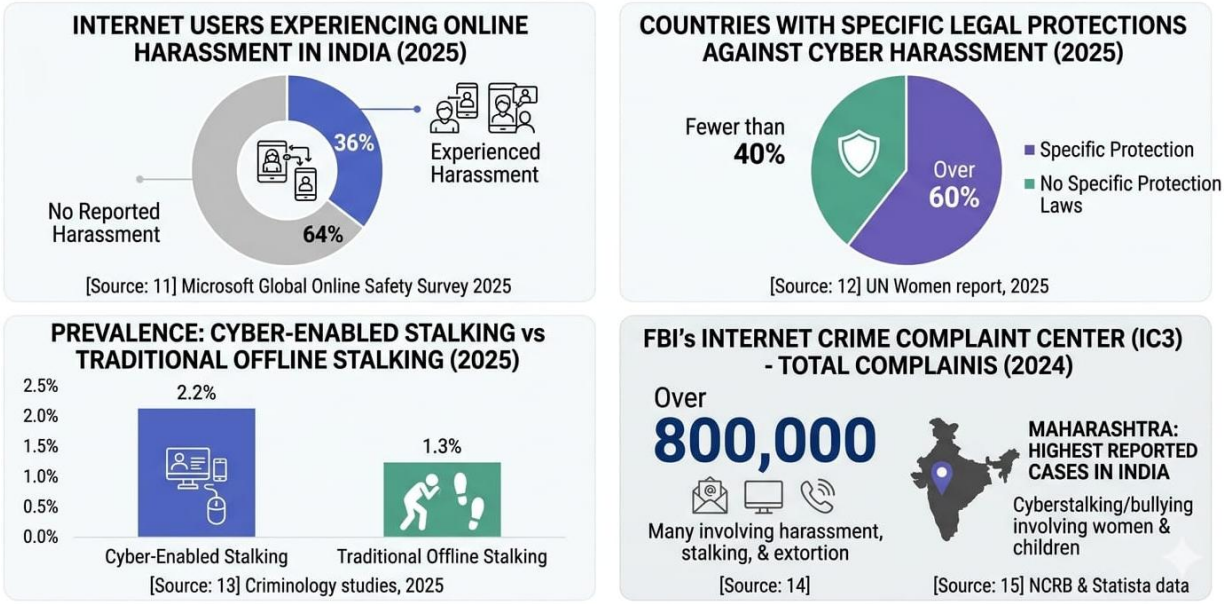

Figure 1: Key Statistics on Cyberstalking and Online Harassment

Latest data shows how serious the problem of cyberstalking and online harassment has become. According to the Microsoft Global Online Safety Survey 2025, around 36% of internet users in

[6] Madhumitha Gopinath, 'Reconceptualising Cyberstalking Regulation in India' (2026) 12(1) International Journal of Law 383, 384 (noting anonymity as the defining structural feature of cyberstalking).
[7] Ankita and Dr Parvinder Kaur, 'Digital Abuse in India: A Legal Examination of Cyber Stalking and Online Harassment Under the IT Act, 2000' (2025) 13(5) IJCRT d758, d759–d760.

India reported experiencing some form of online harassment or cyberbullying.

Globally, the legal response is still limited. A UN Women report from 2025 notes that fewer than 40% of countries have specific legal protections against cyber harassment, which leaves many victims without clear legal remedies.

Research in criminology studies from 2025 also shows that cyber-enabled stalking cases, about 2.2%, have now exceeded traditional offline stalking, which stands at around 1.3%.

In terms of reporting, the FBI's Internet Crime Complaint Centre recorded more than 800,000 cybercrime complaints in 2024, many involving harassment, stalking, and online extortion.

Within India, Maharashtra has reported the highest number of cyberstalking and cyberbullying cases involving women and children, according to NCRB and Statista data.[8]

C. Typology of Cyberstalkers: A Criminological Approach

The Mens Rea (guilty mind) of cyberstalkers can be better understood by employing a Typology of Cyberstalkers, which is a very academic approach to what you do.

- **The Obsessive/Erotomanic Stalker** - Their motivation is a delusional belief that the victim is in love with them. They believe that the victim's actions of "blocking" or "rejection" are a "test of love" and therefore create multiple profiles to stay in touch with the victim.
- **The Revenge/Rejected Stalker** - Typically a past romantic interest or acquaintance of the victim, who seeks to punish the victim for a real or imagined grievance or for the termination of the relationship.
- **The Predatory Stalker** - The most dangerous of all cyberstalkers, as their motivation is to gather information to facilitate a future physical or sexual assault against the victim.
- **The Political/Ideological Stalker** - A relatively new phenomenon, wherein the cyberstalker seeks to victimize a person for their political or ideological beliefs, which can manifest as a "dogpiling" or "doxxing" of the victim.[9]

III. LEGAL FRAMEWORK IN INDIA

In India, the regulation of cyberstalking is governed under a mix of legislative, penal, and

[8] *NCRB data shows rise in cybercrimes using mobile phones and computers: DD News On Air* (no date) *Newsonair*. Available at: https://www.newsonair.gov.in/ncrb-data-shows-rise-in-cybercrimes-using-mobile-phones-and-computers/ (Accessed: 09 April 2026).

[9] *Cyberstalking facts - types of stalkers and Cyberstalkers* (2025) *iPredator*. Available at: https://ipredator.co/cyberstalking-facts/ (Accessed: 09 April 2026).

intermediary laws, rather than any single legislation. The idea behind this fragmented approach is to address the different facets of cyberstalking, which include identity theft, cyber harassment, violation of privacy, and transmission of harmful content, among others. Nevertheless, the lack of any legislation dealing exclusively with cyberstalking remains a challenge. The approach to the regulation of cyberstalking in India has been gradual, with changes made to existing laws.

A. Information Technology Act, 2000

The Information Technology Act, 2000, along with the amendment made in 2008, is the backbone of cyber law in India, which offers many provisions that can be indirectly applied in the context of cyberstalking.

Firstly, the Information Technology Act, 2000, under Section 66C, prohibits identity theft, which includes the fraudulent use of another person's electronic signature, password, or unique identification feature. In the case of cyberstalking, the stalker often creates fake profiles or hacks the account of the victim and poses as the victim, which falls under the jurisdiction of this section.

Secondly, the Information Technology Act, 2000, under Section 66D, prohibits cheating by personation using computer resources, which is applicable in the case of cyberstalking, where the stalker often cheats others by assuming the identity of the victim or creating fake digital identities.

Lastly, the Information Technology Act, 2000, under Section 66E, prohibits the violation of privacy, which includes the capture, publication, or transmission of images of a person's private areas without his/her consent. In the case of cyberstalking, the stalker often sends images that violate the privacy of the victim.

Moreover, the Information Technology Act, 2000, under Sections 67 and 67A, prohibits the publication or transmission of obscene and sexually explicit content in electronic form, which is applicable in the case of cyberstalking, where the stalker often sends images that contain defamatory, obscene, and morphed content.

Lastly, the Information Technology Act, 2000, under Section 72, along with Section 72A, prohibits the breach of confidentiality and the unauthorized disclosure of personal information, which protects the sensitive data of the victim from being misused in the cyber environment.

Although the Information Technology Act, 2000, offers many provisions that can be indirectly applied in the context of cyberstalking, the provisions are offence-specific rather than behaviour-specific, which results in a fragmented approach rather than defining the offence of

 [ISSN 2581-5369]

cyberstalking.[10]

B. Bharatiya Nyaya Sanhita, 2023 (Earlier IPC Provisions)

The implementation of the Bharatiya Nyaya Sanhita, 2023 (BNS) has greatly modernized the provisions of the law relating to cyberstalking. This is particularly evident in the implementation of Section 78 of the Bharatiya Nyaya Sanhita, 2023, which replaces the provisions of Section 354D of the Indian Penal Code, 1860.

The new provision of the Bharatiya Nyaya Sanhita, 2023, has clearly defined the crime of stalking, which includes the monitoring of the internet or electronic communication of a person. This is a major shift in the implementation of the law relating to stalking, as the new provision recognizes digital stalking as part of the crime. This bridges the gap between physical and cyberstalking.

The new provision of the Bharatiya Nyaya Sanhita, 2023, also recognizes repeated attempts to contact or to monitor the online activities of a person who has clearly expressed disinterest. This is particularly evident in the implementation of the law relating to the stalking of people through social media platforms.

The provisions of the law relating to criminal intimidation, defamation, and insult to modesty also form part of the law relating to cyberstalking. However, despite the advancement of the law relating to stalking, the new provision of the Bharatiya Nyaya Sanhita, 2023, is limited in its scope as it fails to cover complex forms of cyberstalking.[11]

C. Intermediary Liability and IT Rules, 2021

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is of critical importance in the regulation of cyberstalking issues by digital platforms.

In these rules, intermediaries such as social media platforms are required to exercise due diligence and develop a mechanism for the redressal of grievances of users. For this purpose, intermediaries are required to appoint a Grievance Officer to address issues of cyberstalking and other forms of harassment of users within a specified period of time.

It is also mandatory for intermediaries to remove or disable access to unlawful content within 24-36 hours of receiving a valid complaint regarding the same. This is of critical importance in cyberstalking issues involving the dissemination of harmful or defamatory content.

Moreover, intermediaries such as social media platforms are required to develop traceability

[10] Information Technology Act, 2000, §§ 66C, 66D, 66E, 67.
[11] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 78 (India).

 [ISSN 2581-5369]

mechanisms for determining the originator of a message in critical cases, as applicable to intermediaries with significant user numbers. This is of critical importance in cyberstalking issues due to the anonymity of the perpetrator of cyberstalking.

However, there are concerns regarding the privacy of users and over-regulation of intermediaries due to the increased traceability of messages and their potential to violate the right to privacy of users as provided under Article 21 of the Constitution.

In spite of these issues and concerns, IT Rules, 2021 is of critical importance in ensuring the active involvement of intermediaries in the regulation of cyberstalking issues.

D. Digital Evidence and Evidentiary Framework

The regulation of cyberstalking is also heavily influenced by the admissibility of digital evidence, which is subject to the provisions of evidentiary law.

The erstwhile Indian Evidence Act of 1872 provided for the admissibility of electronic records under Section 65B of the Act, which required a certificate to prove the authenticity of such records. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaced the Evidence Act of 1872, provides for a modern framework for the admissibility of electronic records and other digital evidence.

The provisions of the Bharatiya Sakshya Adhiniyam, 2023, emphasize the authentication and reliability of electronic records and other digital information such as data from cloud services, network systems, and other digital devices. The requirement of certification ensures the integrity of electronic records such as screenshots and other digital evidence to prevent their alteration or manipulation.

In the context of cyberstalking cases, digital records such as IP logs and headers of emails and other data become critical to identify cyberstalkers and track patterns of cyberstalking behavior.

Despite these advances in the regulation of cyberstalking and the availability of digital records as critical evidence, technical difficulties and the lack of technical skills of law enforcement officials and the difficulty of accessing data from foreign platforms pose hurdles in investigations and prosecutions of cyberstalking cases.[12]

E. Data Protection and Privacy Framework

The development of data protection laws has also introduced a new dimension to the regulation of cyber stalking, particularly with regard to the misuse of data.

[12] Indian Evidence Act, 1872, § 65B.

 [ISSN 2581-5369]

The Digital Personal Data Protection Act, 2023 has been enacted to regulate data processing and ensure that the data of individuals is handled lawfully and securely. Although not directly addressing the issue of cyber stalking, the Act provides a framework of protection against the misuse of data collection and profiling by stalkers.

The Act imposes obligations on data fiduciaries to ensure data security and accountability, thereby indirectly contributing to the regulation of cyber stalking.

Moreover, the judicial recognition of the right to privacy as a fundamental right under Justice K.S. Puttaswamy v. Union of India also provides a framework for the regulation of cyber stalking by providing a right to privacy.

The interface of data protection and cyber stalking is not well developed, and the existing framework does not directly address online harassment and stalking behaviors.

IV. CASE STUDIES ON CYBERSTALKING

A. Manish Kathuria v. Ritu Kohli

Manish Kathuria v. Ritu Kohli (2001) is the first case worth mentioning. In the case, the accused developed a bogus identity under the name of the victim in an online chat room and posted her telephone number that made her receive a lot of obscene calls. There were no laws regarding cyberstalking in India by that time, and the police were left to apply Section 509 of the Indian Penal Code, which concerns an insult to the modesty of a woman. This case has raised the legal loopholes in the handling of cybercrimes during the early digital age.[13]

B. Suhas Katti Case

In State of Tamil Nadu v. Suhas Katti (2004). The accused left obscene and defamatory messages about a woman on a Yahoo message board. The case gained relevance due to the fact that the court passed a conviction in seven working days thus showing that the current cyber laws could be implemented successfully depending on how they were investigated.[14]

C. Kalandi Charan Lenka

The accused in the case of Kalandi Charan Lenka v. State of Odisha (2017) had falsely created social media accounts and shared obscene images and messages against a woman. The Orissa High Court concluded that this continuous online harassment may constitute stalking and an offense to the modesty of a woman and demonstrated that digital harassment should be

[13] Manish Kathuria v. Ritu Kohli, Delhi Police Cyber Crime Case (2001)
[14] State of Tamil Nadu v. Suhas Katti (2004)

 [ISSN 2581-5369]

considered a serious criminal act in the current legislation.[15]

D. Shreya Singhal

The case of Shreya Singhal v. Union of India (2015) was a significant constitutional change. Here, the Supreme Court declared a Section of the Information Technology Act, 2000, 66A, invalid. Section 66A made it a crime to send online messages that were deemed to be offensive, annoying, or inconveniencing. The Court held that these terms were vague and overly broad, which allowed authorities to misuse the law to arrest people for ordinary online speech. The judgment ruled that Section 66A violated Article 19(1)(a) of the Constitution, which guarantees freedom of speech and expression, and therefore declared it unconstitutional.[16]

Together, these cases illustrate how Indian courts have gradually adapted traditional criminal law to address emerging cyberstalking behaviours in the digital age.

V. THE PSYCHOLOGICAL AND CRIMINOLOGICAL IMPACT OF CYBERSTALKING

Stalking, in the conventional sense, involves physical proximity. However, cyberstalking takes advantage of the omnipresence of the internet, thus creating a condition of perpetual victimization. The psychological impact is also more intense, given the absence of any "safe space" for the victim.

A. Clinical Psychological Manifestations

The psychological impact on the victim is not merely transient, as the experience leads to clinical conditions such as:

Post-Traumatic Stress Disorder (PTSD): The victim is in a condition of perpetual "hyper-vigilance," where the sound of notification flash on the phone or computer will trigger flashbacks or severe anxiety attacks.

Chronic Anxiety and Depression: The perpetual nature of cyberstalking, which may go on for months or years, will inevitably create a condition of learned helplessness, or depression.

Social Withdrawal (Digital and Physical): The victim may be forced to withdraw from social sites, or even physically withdraw from college or work, thus incurring professional or social costs.

B. Vulnerable Demographics: Women and Minors

Gender, being the most significant factor, has made cyberstalking a predominantly female-

[15] Kalandi Charan Lenka v. State of Odisha,2017 SCC
[16] Shreya Singhal v. Union of India, (2015) 5 SCC 1

 [ISSN 2581-5369]

targeting offense, with the effect being varied across demographics:

Impact on Women: In the Indian context, cyberstalking has resulted in the offense of "reputational terrorism," wherein the stalker sends out defamatory matter or obscene morphed pictures with the intent to cause social ostracization. The fear of being victim-blamed has deterred them from seeking legal redress.

Impact on Minors: Children are also vulnerable to the offense of "Cyber-Grooming" or "Cyber-Bullying" masquerading as cyberstalking. Unlike adults, children may not possess the emotional quotient to deal with the trauma of cyberstalking, making them more vulnerable.[17]

C. The Criminological Perspective: Why They Stalk

To understand the Mens Rea (guilty mind), the criminological perspective is pertinent for better legal profiling:

The Power-Reassurance Stalker: The stalker seeks power and control over the victim, who has rejected them, as in the case of an ex-partner.

The Resentful Stalker: The stalker harbors some grudge or grievance, which he uses the anonymity of the Internet to level the playing field with the victim.

The Fantasy-Driven Stalker: He is driven by erotomanic delusions, wherein he believes the victim is in love with him.

D. Victimology: The "Invisible" Victim

As far as victimology is concerned, cyberstalking generates a "Secondary Victimization" effect in that:

The Anonymity Gap: The victim fears the "unknown" perpetrator and believes that everybody in her virtual social circle is a potential threat.

Systemic Failure: When law enforcement fails to treat virtual harassment seriously and treats it as "lesser" than physical threats, the victim feels marginalized and does not report the incident to the authorities.[18]

VI. DIGITAL EVIDENCE AND THE INVESTIGATIVE PROCESS

In cyberstalking cases, the "crime scene" is virtual. This means that the collection and preservation of electronic records are the most important aspects of the litigation process.

[17] 4. Verma A. The Quest for Justice: Cyberstalking Against Women in India. Lex Localis J. of Local Self-Gov't, 2023, https://lexlocalis.org/index.php/LexLocalis/article/

[18] Madhumitha Gopinath, Reconceptualising Cyberstalking Regulation in India, 12 INT'L J. L. 383 (2026)

A. Taxonomy of Digital Evidence

IP Logs and Session Data: This helps investigators identify the physical location and Service Provider (ISP) of the stalker. It provides the unique numerical identifier assigned to a device.

Metadata (The "Data about Data"): This refers to time stamps and geolocation tags in photographs and email headers that reveal the exact time and origin of a harassing message.

System and Application Logs: These are records from social media sites that reveal the victim's social media activities and interactions with the stalker's social media account.

B. Integrity via Hashing and Chain of Custody

Hashing: To ensure that the evidence is not tampered with, the investigators create a unique digital fingerprint of the file using a cryptographic "hash function" like SHA-256. Any change to the file, no matter how small, will change the hash, which will then alert the court to the fact that the evidence might have been tampered with.

Chain of Custody: It is a chronological record of who has handled the digital evidence, how, and when. In the case of cyberstalking, a break in the chain of custody, like the officer accessing the victim's phone without a write-blocker, can lead to the evidence being dismissed.

C. Admissibility: From Section 65B IEA to Section 63 BSA

The Certificate Requirement: Until the Bharatiya Sakshya Adhiniyam, 2023, the Indian Evidence Act required a certificate to accompany the electronic records to prove that the electronic records were produced by a computer in regular use, as prescribed under Section 65B(4) of the IEA.

The BSA Transition: Under the Bharatiya Sakshya Adhiniyam, 2023, the standards for "secondary" electronic evidence are equally stringent. The judiciary is now more concerned with the Certificate of Authentication, which has to be signed by a person in charge of the computer or an expert.

Judicial Precedent: As witnessed in Shreya Singhal v. Union of India, the judiciary is becoming increasingly cautious of "vague" digital evidence that could compromise free speech or even privacy.

VII. CHALLENGES IN ADDRESSING CYBERSTALKING

A. Jurisdictional Problems

Cybercrimes have no geographical boundaries and criminals can be located in various states or

 [ISSN 2581-5369]

countries. A cyber stalker can send threatening messages to a victim in India while being based in a different country. This poses immense challenges in identifying the legal authority with jurisdiction to deal with the offence. Although the Information Technology Act provides for extraterritorial jurisdiction in certain scenarios, these provisions cannot be enforced without international cooperation. The absence of effective extradition treaties and the slowness of international legal processes make it difficult to apprehend offenders.[19]

B. Anonymity and Identity Concealment

Anonymity of online media is a significant impediment in cyberstalking cases. Cyber stalkers tend to conceal themselves behind false identities, pseudonyms, or encrypted communication systems. Tracing the physical identity of the culprit requires complex digital forensic methodology that many law enforcement agencies lack. Even where police can follow an IP address, criminals can use VPN services or public networks to conceal their whereabouts. This renders identification and prosecution highly difficult.[20]

C. Awareness Deficiency Among Victims

A huge proportion of victims of cyberstalking is not willing to report the issue to the police. This could be because of fear of being socially stigmatised, lack of knowledge on available legal redress or fear of additional harassment. In some cases, the victims believe that reporting the crime would make the situation worse or even create undesirable publicity. Consequently, this leads to numerous cases of cyberstalking remaining unreported and hence, it is hard to determine the true scale of the issue.

D. Technological and Investigative Restrictions

Cyberstalking cases require highly specialised technical and electronic forensics. Law enforcement agencies should be in a position to decipher digital evidence such as emails, social media messages, IP addresses and electronic records. However, not all the police departments possess sufficient technical training and capabilities to deal with sophisticated cybercrimes. Gaining access to information in foreign online sources can be both costly and time-consuming due to legal and formalities, which leave the perpetrator time to erase traces or keep harassing their victims.[21]

[19] IT Act, 2000, s. 75 (extraterritorial jurisdiction); Rodrigues (n 2) 579–580 (discussing the practical limitations of enforcement across jurisdictions).
[20] Heena Keswani, 'Cyber Stalking: A Critical Study' (2017) Bharati Law Review.
[21] 20. U.S. Agency for International Development.
https://www.usaid.gov/digital-policy

E. Inadequate Legal Provisions

Although there are several statutory provisions, Indian law has no specific legislation to deal with cyberstalking. This leaves prosecutors with no choice but to use a combination of various legal provisions and hence inconsistencies in the interpretation of the law. According to legal experts, the issue of cyberstalking needs a specific and an elaborate piece of legislation that would explicitly capture the technological aspects of online bullying. A proper legal system should be supported by preventive strategies to reduce the target suitability of the possible victims.[22]

VIII. PREVENTIVE MEASURES AND CYBER SAFETY ECOSYSTEM

A sound legal framework must be accompanied by preventive measures to deter the "target suitability" of potential victims.

A. Personal Safety and Digital Hygiene

Multi-Factor Authentication: Using 2FA will provide an additional layer of protection so that even if stalkers obtain the password of personal online accounts, they will still not be able to log in.

Granular Privacy Settings: Auditing "Audience" settings in social media sites to ensure that photos posted with location tags and personal information such as DOB and phone numbers are restricted from public view.

Digital Footprint Management: Periodically "Googling" oneself to check what information is available online and requesting the removal of such information via "Right to be Forgotten."

Illustrations:

Practical safety measures are the first line of defense against cyber stalkers. The examples below illustrate how a potential victim can "harden" his/her digital presence to prevent stalking or harassment.

- Preventing "Location Stalking"

The Scenario: The stalker uses the victim's Instagram posts to show up at cafes or parks where the victim goes to spend time.

The Hygiene Practice: The victim should disable "Precise Location" permission for social media applications in the phone's settings.

[22] Shreya Singhal v Union of India (2015) 5 SCC 1 (striking down s. 66A IT Act for vagueness); Gopinath (n 4) 389–390 (advocating a dedicated cyberstalking statute).

Advanced Step: The victim can use "Delayed Posting," where he/she shares photos of the location only after he/she has left that location.

- Securing Against Account Takeover

The Scenario: The ex-partner tries to guess the password or use "forgot password" options to gain access to the victim's personal emails.

The Hygiene Practice: The victim can use Multi-Factor Authentication (2FA) through an authenticator application instead of SMS.

Advanced Step: The victim can use a password manager to create complex passwords of 16 characters and alphanumeric values for all accounts so that an account breach on one site does not lead to compromised accounts on other sites.

- Auditing the "Digital Footprint"

The Scenario: A stalker discovers the old location of a victim or the names of the victim's family members from an archived blog or the victim's old Facebook profile.

The Hygiene Practice: Conducting a "Privacy Audit" by searching for one's name on multiple search engines and using the "View As" feature on Facebook to see what a stranger can see.

Advanced Step: Submitting a "Right to be Forgotten" request to the search engines to remove old personal information that can be used for "doxxing".

B. Institutional and Government Initiatives

Dedicated Cyber Cells: All states in India have Cyber Crime Police Stations to tackle high-tech harassment.

National Cyber Crime Reporting Portal (cybercrime.gov.in): A central government initiative to allow victims of cyber stalking to file a complaint anonymously, especially for crimes against women and children.

I4C (Indian Cyber Crime Coordination Centre): An apex organization constituted by the Ministry of Home Affairs to facilitate coordination between state police forces and international organizations to tackle international stalking.

C. Role of Intermediaries

Notice and Takedown: The IT Rules 2021 mandate the appointment of a Grievance Officer by social media companies to tackle stalking and harassment complaints within 24-36 hours.

AI-Driven Filtering: Social media companies are employing "Proactive Monitoring" tools to detect and remove offensive posts or images from the platform to avoid the victim from seeing

 [ISSN 2581-5369]

the offending material.[23]

IX. FINDINGS/RESULTS

First, cyberstalking is rapidly becoming a significant cybercrime owing to the growing use of digital communication technology. Online communication tools and social media have greatly facilitated the ability of perpetrators to track, threaten, and harass their victims.

Second, cyberstalking has severe psychological and emotional consequences for victims. Constant online harassment is associated with anxiety, depression, isolating behaviour, and reputational damage. Digital harassment differs from conventional harassment in that it can persist longer and reach a much larger audience.

Third, the legal system in India is fragmented and lacks specific reference to cyberstalking, although there are some legal provisions that are used to combat cyber offences. The provisions of the Information Technology Act and the criminal law address only a few aspects of cyber harassment without offering a comprehensive remedy.

Fourth, as it can be seen based on the case law, Indian courts are starting to recognize the seriousness of cyberstalking. The Manish Kathuria v. Ritu Kohli, State of Tamil Nadu v. Suhas Katti and Kalandi Charan Lenka v. State of Odisha cases demonstrate that the judicial system is ready to punish those who exploit digital channels to inflict harm on their victims.[24]

Fifth, cyberstalking law has a weakness of being difficult to enforce due to jurisdiction, anonymity of offenders, technical constraints and underreporting by victims. Cyberstalking will continue to be a significant challenge in cyberspace until they are dealt with by reforming the law and enhancing investigative ability.

X. POLICY RECOMMENDATIONS AND REFORMS

A. Enactment of Specific Legislation on Cyberstalking

India requires a dedicated, comprehensive law specifically addressing cyberstalking. Currently, cyberstalking is governed by a mix of provisions from the Information Technology Act, 2000, and criminal law, which were primarily designed for offline offences and are inadequate to handle the intricacies of digital harassment. A standalone statute should provide a clear, technology-neutral, and gender-neutral definition of cyberstalking, explicitly cover modern forms of digital abuse such as doxxing and deepfake harassment, and introduce digital

[23] 6. Banerjee P, Banerjee P. Analysing the Crime of Cyberstalking as a Threat for Privacy Right in India. Academia, 2022.
[24] Manish Kathuria v Ritu Kohli, Delhi Police Cyber Crime Case (2001); State of Tamil Nadu v Suhas Katti (2004); Kalandi Charan Lenka v State of Odisha 2017 SCC OnLine Ori 397.

protection orders that courts may issue at the outset of proceedings.[25]

B. Enhancing Cybercrime Investigation Capacity

Cyber laws require specialised enforcement tools. Law enforcement agencies should be provided with enhanced digital forensic equipment and trained personnel to handle cyberstalking cases. The establishment of dedicated cybercrime departments in police stations across the country would go a long way in improving the investigation and prosecution of cyberstalking offences.

C. Enhancing Awareness and Digital Literacy

The major challenge in the fight against cyberstalking is the lack of knowledge of most internet users on cyber safety and legal protection. Many victims do not report cyber harassment due to fear, social stigma, and lack of awareness of available legal protection. Law enforcement and learning institutions ought to implement awareness programs to inform individuals about internet safety and privacy settings as well as how to report cybercrimes.

D. Greater Regulation and Accountability of Social Media Platforms

Social media platforms are being used more and more to cyber harass. These sites should be compelled to have more vigorous monitoring strategies to detect and eliminate malicious content in time. They are also expected to provide easy reporting channels where victims can easily report cyberstalking. To curb the abuse of online platforms, technology firms should cooperate with the law enforcement agencies to assist in the detection of criminals.[26]

E. International Cooperation in Cybercrime Investigation

Cyberstalking crimes frequently involve offenders who are located in various jurisdictions and thus, international collaboration is invaluable in effective law enforcement. The international cooperation against cybercrime should be enhanced by increasing the strength of the existing international agreements, as well as the extradition processes, in order to ensure that the criminals working in other jurisdictions can be taken to justice. India also needs to contemplate joining the Budapest Convention on Cybercrime to enable a well-organized cross-border collaboration.

XI. CONCLUSION

Cyberstalking is now a major cybercrime in the current digital age. The intensive spread of

[25] Criminal Law (Amendment) Act, 2013, No. 13 of 2013 (inserting s. 354D IPC); now re-enacted as s. 78, Bharatiya Nyaya Sanhita, 2023; Gopinath (n 4) 391.
[26] Chandra A. Privacy and the Indian Constitution after Puttaswamy. Indian J. Const. L.,2017:9:1.

internet technologies and social media has made people increasingly susceptible to cyber harassment and abuse. The effects of cyberstalking are not only devastating on the privacy of the people but also devastating psychologically and emotionally to the victims.

An overview of the legal provisions and case law indicates that India has made certain efforts to fight cyberstalking under the Information Technology Act, 2000, and criminal law of stalking and harassment. Nevertheless, these legal frameworks are still not comprehensive and do not offer a full solution to the issues of cyberstalking on the internet. As the cases of Manish Kathuria v. Ritu Kohli, State of Tamil Nadu v. Suhas Katti and Kalandi Charan Lenka v. State of Odisha indicate, the Indian courts are slowly beginning to regard cyberstalking as a serious crime against personal dignity and privacy. Similarly, the decision in Shreya Singhal v. Union of India highlights the importance of the need to strike a balance between cyber regulation and the fundamental right to free speech and expression.

The issue of cyberstalking can only be solved through a complex approach that includes enhanced specialized laws, better tools to investigate cybercrimes, more awareness of the masses, and effective international cooperation. These changes will assist in making India a safer online environment and guarantee better security of individuals in regard to cyber harassment during the digital age.

*****

 [ISSN 2581-5369]

XII. REFERENCES

Books and Articles

- Rodrigues, V., 'Cyber Stalking: Issues of Enforcement in Cyber Space' (2020) 3(2) International Journal of Law Management & Humanities 568.
- Gopinath, M., 'Reconceptualising Cyberstalking Regulation in India: From a Disjointed Legal Framework to Proactive Digital Safety Governance' (2026) 12(1) International Journal of Law 383.
- Agnihotri, U. and Thapak, N.K., 'The Cyberstalking Situation in India: A Social, Legal, and Technological Viewpoint' (2024) 15 Purva Mimaansa 34.
- Ankita and Kaur, P., 'Digital Abuse in India: A Legal Examination of Cyber Stalking and Online Harassment Under the IT Act, 2000' (2025) 13(5) International Journal of Creative Research Thoughts d758.
- Keswani, H., 'Cyber Stalking: A Critical Study' (2017) Bharati Law Review (Apr–Jun) 131.
- Rachna and Varshney, R., 'Cyberbullying and Cyberstalking Laws in India: Legal Safeguards Against Online Harassment' (2024) 27(5S) African Journal of Biomedical Research 799.
- Chandra A. Privacy and the Indian Constitution after Puttaswamy. Indian J. Const. L.,2017:9:1.
- Banerjee P, Banerjee P. Analysing the Crime of Cyberstalking as a Threat for Privacy Right in India. Academia, 2022.
- Verma A. The Quest for Justice: Cyberstalking Against Women in India. Lex Localis J. of Local Self-Gov't, 2023.

Statutes

- Information Technology Act, 2000, No. 21 of 2000.
- Information Technology (Amendment) Act, 2008.
- Indian Evidence Act, 1872.
- Criminal Law (Amendment) Act, 2013, No. 13 of 2013.
- Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023.

Case Laws

- Manish Kathuria v. Ritu Kohli, Delhi Police Cyber Crime Case (2001).
- State of Tamil Nadu v. Suhas Katti (2004) Cybercrime Conviction Case.
- Shreya Singhal v. Union of India (2015) 5 SCC 1.
- Kalandi Charan Lenka v. State of Odisha, 2017 SCC OnLine Ori 397.

*****

 [ISSN 2581-5369]