



## Cyberstalking in the Contemporary Society

*Agnel Sherin J*

*B. Com, LLB (Hons) The Tamil Nadu Dr. Ambedkar Law University, India*

### ABSTRACT

Cyberstalking is an emerging form of cyberterrorism crime. Although it frequently receives less attention than cyber terrorism, it is nonetheless a significant global issue. It is affecting people in many ways as a result of new technologies. It is spreading swiftly because of the anonymity and security that the Internet offers. As a result, the Internet has effectively developed into a fertile breeding ground for a brand-new and distinct category of criminal offenders known as cyber stalkers. A cyber stalker is a criminal who employs sophisticated stalking techniques to prey upon, harass, threaten, and greatly increase the fear and trepidation in their victims by using the Internet as a tool or weapon. This article's goal is to investigate the concept and definition of cyberstalking as well as to examine the numerous legislative measures intended to combat it in the Indian legal system. It also focuses on relevant cases of stalking on the Internet and the decisions taken by the judiciary. This article also makes recommendations for how to assist victims of online stalking.

**Keywords:** Cyberstalking, Cybercrime, Cyber security, Internet

### 1. Meaning and Definition of Cyberstalking

Almost every element of civilization has advanced thanks to the Internet's explosive growth in this millennium, and it is now available and usable almost everywhere in the world. The expected societal advantages are enormous. The Internet is principally responsible for expanding and enhancing international trade to levels that were previously unthinkable, promoting amazing improvements in healthcare and education, and facilitating communication between nations that were formerly thought to be expensive and limited. With its infinite size and previously unheard-of capabilities, the Internet does, however, have a dark side in that it has created previously unheard-of criminal opportunities that not only challenge but also transcend all geographical boundaries, borders, and restraints to identify, punish, and lessen what appears to be a major social issue on a global scale. The Internet has evolved into the perfect tool for people who want to intimidate, threaten, and harass others because it allows human interaction without the restrictions of physical barriers and with the perception of anonymity. Under the pretext of a fictional screen name or pseudonym, a stalker can utilize the Internet to send ominous messages to anybody, anywhere, in a matter of seconds.

Although the term "cyberstalking" has no universally accepted definition, it typically refers to the use of the internet or other telecommunications technologies to harass or threaten another person. Although the behaviour that is commonly known as stalking has existed for generations, the legal system has only recently defined its existence in the laws. The use of electronic communication, such as pagers, mobile phones, e-mails, and the Internet, to bully, threaten, harass, and intimidate a victim is known as cyberstalking.

Expert on offline stalking in the United States, Meloy, contends that the word "cyberstalking" implies,

*"a paranoid tinged world of malicious and intrusive activity on the Internet"*

The following is Meloy's explanation of cyberstalking:

When stalking someone online, there are two illegal purposes that might be accomplished:

1. To obtain intimate information about the target in order to intensify a quest; and
2. To converse with the target either implicitly or overtly, in order to intimidate or frighten them.

Meloy's definition is intriguing since it permits behaviours like data theft, in which a person uses the Internet to obtain victim information. Furthermore, Meloy does not focus primarily on e-mail as the means of communication between the harasser and the victim and takes into account relatively recent developments like instant messaging. Meloy's definition is unquestionably concise, but it doesn't seem to be all-inclusive. For instance, it doesn't specifically address some of the practices involved in cyber-stalking, like real-time monitoring.

The use of thresholds becomes considerably more challenging to support in the context of cyberstalking. It is feasible, for instance, for a cyberstalker to employ software that sends messages automatically over time. Once the software is set up, a threatening or abusive message could be delivered every day, every week, or every month without the harasser's additional involvement. It is unclear in this instance whether this activity is considered to be a single incident or a collection of separate episodes.

In some definitions, cyberstalking is solely discussed in terms of its typical behavioral patterns, for instance,

according to Ellison and Akdeniz :

*“The term cyberstalking is online harassment, which may include various digitally harassing behaviors, including sending junk mails, computer viruses, impersonating the victim, etc.”*

Although there is no doubt that this definition is helpful, it only discusses a handful of the behaviours that are frequently observed in cyberstalking instances and leaves out an explanation of what is meant by "harassment."

Many people mistakenly believe that cyberstalking involves a sexual preoccupation because it is commonly misconstrued; nevertheless, the research findings are not as conclusive in that aspect. Instead of being driven by money or a sexual obsession, Mustaine and Tewksbury argue that stalking is a crime driven by interpersonal antagonism and aggressive behaviours resulting from power and control difficulties. Like conventional offline stalking, cyberstalking is motivated by rage, power, control, and anger that may have been sparked by the victim's deeds. According to the research, there will probably be a rise in the number of cyberstalking cases, in part because the Internet provides an anonymous haven where an offender may potentially hide and disguise one's identity. Offenders can communicate with virtually anybody who has access to the Internet anytime, with minimal risk of being discovered and considerably less concern about being detained and facing legal action in many places.

---

## 2. Existing Legal Provisions

In India, cyberstalking is punishable under the following legal provisions:

1. Indian Penal Code 1860
2. The Information Technology Act 2000

### **INDIAN PENAL CODE**

#### **SECTION 354D**

After the Delhi Gang Rape case in 2012, the Justice Verma committee enacted the Criminal Law Amendment Act in 2013, which amended the Indian Penal Code. After the Delhi Gang Rape case in 2012, the Justice Verma committee enacted the Criminal Law Amendment Act in 2013, which changed the Indian Penal Code. Stalking has been classified as a crime under section 354D, both offline and online. The 353–357 section of the IPC contains India's rules against stalking. In India, cyberstalking is not, however, expressly made illegal by law. The section is as follows:

*(1) Any man who*

- i. 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*
- ii. monitors the use by a woman of the internet, email or any other form of electronic communication commits the offence of stalking.*

#### **ISSUES**

##### **GENDER DISPARITY**

As the part exclusively mentions women being stalked while ignoring the reality that males can also become victims, there is an issue of equality at play here. The notion that only a boy or man would stalk a girl or woman is easily disproven. As a result, the legislation is gender biased.

##### **MEANS OF MONITORING**

The "method of monitoring" has not been acknowledged by lawmakers. It is possible for someone to act in a stalker manner without intending to do so.

##### **BAILABLE OFFENCE**

When committed for the first time, the stalking offence under section 354D is cognizable and subject to bail; however, for successive offenses, the offence is no longer subject to bail and carries a harsher penalty. It is important to remember that a subsequent offence is only taken into account after a conviction for the preceding offence.

It is actually quite necessary to make it non-bailable since individuals frequently abuse it. In addition to being illegal on its own, stalking frequently serves as a pretext for additional crimes, most notably sexual harassment.

#### **SECTION 503**

Section 503 of the Indian Penal Code, 1860 defines Criminal Intimidation as:

*"Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of anyone 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."*

This section also addresses instances of criminal intimidation where the perpetrator threatens the victim online. Due to the need in Section 503 that the threat be made known to the target, regardless of the channel, a threat made via social media will still be considered criminal intimidation under Section 503.

## ISSUES

### DIFFICULTY IN ESTABLISHING INTENTION

According to Section 503, the threat must be made with the goal that the target of the threat will learn about it. But through social media, a message meant for a small group might reach millions. Therefore, the law no longer regards it as criminal intimidation when the threat does reach the person who is being threatened but there was no purpose on the part of the accused to actually transmit the threat to the threatened. Further, while communicating online, a person's intent sometimes gets lost in translation. Inappropriate and offensive jokes are frequently seen on social media. It might be challenging to determine whether the accused made a humorous comment or a real threat in many situations.

### SECTION 507

Crimes of "criminal intimidation by anonymous communication" are covered under Section 507 of the IPC. According to this provision, it becomes an offence when a stalker makes an effort to conceal his identity so that the victim is uninformed of the source of the threat. Thus, it provides anonymity, which is a key component of cyberstalking. If the stalker makes an effort to hide their identity, they will be found guilty under this provision.

### SECTION 509

The purpose of Section 509 of the IPC was to safeguard a woman's chastity and modesty. It reads as follows

*"Word, gesture, or act intended to insult the modesty of a woman. —Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both"*

## ISSUE

### CYBERSTALKING IS EXCLUDED FROM ITS PARAMETER

It is a requirement of this section that the actions should be done physically. However, it omits any online activities like cyberstalking when neither the hearing nor the sight senses may be used as described in the preceding section.

### GENDER DISCRIMINATORY

It ignores the reality that men may also become victims of cyberstalking, which is a crime that knows no boundaries between genders.

### SECTION 292

Section 292 of IPC defines "obscenity"

When a stalker attempts to deprave the other person by sending any obscene material on the internet with the intention that the other person would read, see, or hear the content of such material, he is guilty of the crime. This includes sending vulgar materials to the victim via social media, emails, messages, etc.

## INFORMATION TECHNOLOGY ACT, 2000

### SECTION 66E

Voyeurism is a paraphilia that involves getting a sexual high from watching unaware others strip, get naked, or engage in sexual behaviour. The Information Technology Act, of 2000 covers voyeurism. The stalker, as an attempt to dishonour the chastity of the victim, posts personal images of their victims online. Such cyberstalking-led voyeurism is covered under Section 66E of the Act. The section criminalizes the recording, publication, and invasion of a person's privacy.

### SECTION 66A

Section 66A of the IT Act 2000 addresses "punishment for sending offensive messages through communication services, etc." Under this provision, a penalty of up to three years in jail may be imposed on any person, male or female, who transmits an insulting message via a communication medium that results in fear, irritation, hurt, insult, or other harm. This section was removed after the case of Shreya Singhal vs. U.O.I.

### SECTION 67

---

Publishing obscene content in electronic form is addressed in Section 67 of the Information Technology Act. This legislation has been construed to make it illegal to upload pornographic material online. The stalker will be charged with an offence under Section 67 of the IT Act if he attempts to broadcast any lewd information about the victim in electronic form on social media.

#### **SECTION 67A**

According to Section 67A any publication, transfer, or inducing the transmission of materials containing sexually explicit acts is punished by up to five years in jail and a fine for a first offense, and up to seven years in prison and a fine for a second offence.

---

### **3. How To Act Against Cyberstalking: A Procedure**

Since they are committed across all geographical boundaries, cybercrimes are not subject to any particular jurisdiction. Therefore, regardless of where a cybercrime was committed, you can report it to the cybercrime units of any city. The first step is to file a written complaint with the local Cyber Crime Cell. In the written complaint, the complainant must provide their name, contact information, and address. After that, the complainant must send a written complaint to the head of the city's cybercrime cell. If the complainant does not have access to any of the existing cyber cells in India, they may also file an FIR at the closest police station.

The National Commission for Women accepts complaints against stalking. The Commission raises the issue with the police and has the investigation started right away. To further the investigation in cases of serious offenses, the commission may establish an inquiry committee to look into the situation, conduct spot investigations, gather information, interview witnesses, summon the offender and review police files, etc.

The majority of social media platforms provide a reporting mechanism. The IT (Intermediary Guidelines) Rules, 2011, require these websites to take action within 36 hours to remove information related to offensive content. The intermediary must keep these details and any related documents for at least 90 days in case an investigation is needed. Any offensive content that is hosted, stored, or published on the affected person's computer system can be reported to the intermediary in writing or through an email that has an electronic signature.

The Indian Computer Emergency Response Team (CERT-IN) has been designated as the national nodal agency for addressing the issues occurring in tandem with computer security threats by the Information Technology Amendment Act of 2008. They publish guidelines for, among other things, handling, preventing, reporting, and responding to cyber incidents.

---

### **4. Recent Case Laws**

The first documented instance of cyberstalking in India was the case of *Manish Kathuria v. Ritu Kohli* [1]. Manish Kathuria, the accused, was following Ritu Kohli. He sent vulgar texts to people while posing as her. He made the victim's address and phone number public. She started getting inappropriate texts from others. He was charged with violating IPC section 509. Since then, the nation has seen many examples of cyberstalking, and it seems there will never be an end to it.

*Karan Girotra vs. State & another* [2] is another case that touches on the offence of cyberstalking. The woman in this case, Shivani Saxena, petitioned for a divorce by mutual consent in accordance with the Hindu Marriage Act of 1955 because her marriage was not fully consummated. She then met Karan Girotra through online talking on the internet and made a marriage proposal to him. Saxena was invited to Girotra's home under the guise of presenting her to his family. There, Girotra attempted to drug her and sexually abuse her, which he was successful in doing. Girotra began emailing her explicit photos from the night of the assault. In order to force her to marry him, he began threatening to spread lewd pictures of her. With reference to the IT Act, Section 66-A, Saxena filed a complaint.

*State of Tamil Nadu v. Suhas Katti* [3] was the first in India to be decided under Section 67 of the Information Technology Act. The victim was the subject of numerous obscene, defamatory, and vexatious remarks posted on a Yahoo messaging cluster. On filing a single FIR, the perpetrator, who was formerly a family member of the victim, was arrested and found guilty of the crimes listed in IPC Sections 469, 509, and IT Act Section 67

---

### **5. Conclusion and Suggestion**

Since cyberstalking is primarily a psychological crime, it must be addressed through a process of rehabilitation and a therapeutic jurisprudential approach. The victims may be stopped from harming themselves more while fleeing their stalkers if restorative justice is incorporated into the rules governing cyberstalking. The victim's damage may also be repaired by incorporating not just the offender but also the online service providers as part of the restorative process. By educating the perpetrator about the illegality of his activity during the cyberstalking, the laws that make it a crime may inspire remorse in the offender.

In various respects, how closely cyberstalking resembles traditional stalking practices in the real world will determine how much it can be controlled and addressed by the criminal justice system. The new technologies are so different from the old ones that the previous tactics might no longer be applicable, and we might need to reevaluate the nature of the prospective intervention strategies. In conclusion, new and creative legislative, technical, and investigative countermeasures will very probably be required, even though some of the conventional approaches to combating cyberstalking will still be appropriate.

---

India's regulations surrounding cyberbullying and stalking are not up to date in today's reality. Following the Nirbhaya rape event, numerous changes have been made to the penal code, including the (IPC) Indian Penal Code, (CRPC) penal Procedure Code, and (IT) Information Technology Act. The Justice J.S. Varma committee played a significant role in the implementation of numerous criminal legislations, including 354A, 354B, 354C, and 354D, which deal with the stalking of women.

However, these rules and modifications are only partially effective because they don't cover transgender or male stalking. And since there are no effective extradition rules, there is no law if the stalker is a foreign national.

Now that stalker behaviour is being recognized as a public issue that needs to be addressed, jurisdictions all over the world are starting to use the legal system to combat it. An individual may experience behavioural, psychological, and social repercussions as a result of stalking.

It is consequently in the interests of the authorities to act quickly when instances are presented to them since these consequences have the potential to inflict on society. Only by continuing to research the issue will one become more prepared to handle specific issues when they are brought up.

#### **REFERENCES**

---

[1] <https://www.legalindia.com/tag/ritu-kohli-case/>

[2] 2012 SCC OnLine Del 2673.

[3] <https://www.lawmantra.co.in/tamil-nadu-v-suhas-katti-2004-case-related-to-the-posting-of-obscene-messages-on-the-internet/>