



## Cyberstalking and its Legal Aspects: An Analysis

Udit Agnihotri, Research Scholar, Department of Legal Studies  
LNCT University, Bhopal, Madhya Pradesh, INDIA

### ORIGINAL ARTICLE



**Author**  
**Udit Agnihotri**

shodhsamagam1@gmail.com

Received on : 04/11/2023

Revised on : ----

Accepted on : 11/11/2023

Plagiarism : 04% on 04/11/2023



Plagiarism Checker X - Report  
Originality Assessment

Overall Similarity: **4%**

Date: Nov 4, 2023

Statistics: 83 words Plagiarized / 2196 Total words

Remarks: Low similarity detected, check with your supervisor if changes are required.



### ABSTRACT

Cyberspace is witnessing the emergence of a new type of criminality: persistent attempts to contact someone that makes them feel uncomfortable. This new offence is referred to as "cyber stalking." The author has sought to address the issue of cyberstalking, a freshly established phenomenon. After talking about cyberstalking, the author clarifies the differences between it and physical stalking. The Information Technology Act of 2000 and the Indian Penal Code of 1860 are the two legislative provisions that the author of this paper will discuss in great detail. It is imperative to elucidate the limitations of these clauses and their correlation with cyberstalking. Concerns of jurisdiction and enforcement in relation to cyberstalking will also be covered in this lecture. Since "prevention is better than cure," the author will offer some suggestions and preventive actions that people can take before the study ends.

### KEY WORDS

Cyberspace, Identity Theft, Harassment, Anonymity, Psychological Suffering.

### INTRODUCTION

The term "cyberstalking" refers to the criminal activity of a stalker using social media and other online networks to conduct illegal and unlawful monitoring. Stalking is defined as unwelcome and/or persistent observation of another person by an individual or group under section 354D of the IPC. It frequently has to do with intimidating and harassing the victim, and it could involve spying on them and physically pursuing them. The term "stalking" alone denotes illegitimacy, which makes it a terrible crime. As such, cyberstalking automatically qualifies as a serious offence.

The word “cyber” refers to anything having to do with computers or computer networks, such as the internet, but the phrase “stalking” relates to the unlawful act of watching someone. This word doesn’t convey a really novel idea. Both the idea and the practise of online interaction and communication emerged as the field of interaction and communication advanced.

## **Legislative Framework and its Shortcomings**

In this section, the author will focus on the legislative provisions present in Indian legislation, specifically in relation to the Information Technology Act of 2000 and the Indian Penal Code of 1860. The relationship between these clauses and cyberstalking, as well as the specific sections that permit charging offenders, must be explained. Legislators in India view women as the weaker members of society, which leads them to focus every statute on protecting women. This results in gender-biased legislation. There are no provisions that directly address cyberstalking. However, the author has made an effort to provide clarification on a few sections of the Information Technology Act and the Indian Penal Code that are relevant to this offence. The clarification has been given regarding. Let’s get into more detail about the cyberstalking regulations in India:

The first definition of “stalking” is found in IPC Section 354D. It says thus in its entirety:

Stalking occurs when a person tracks down a woman and makes repeated attempts to establish personal contact with her, even when the woman makes it obvious that she is not interested; or when a person keeps an eye on how a woman uses the internet, email, or any other electronic communication tool;

The section was inserted by the Criminal Amendment Act of 2013 in response to the Delhi gang-rape case. This section addresses stalking in both its conventional and online manifestations. The variety of behaviours that make up the “stalking” crime is described in this section. It’s clear from the Section that attempting to monitor a woman’s online activities would be seen as stalking. Therefore, if the stalker participates in any of the behaviours specified in Provision 354D of the Indian Penal Code, he will be held guilty of an offence under that section.

This section has a lot of mistakes. Firstly, it ignores the notion that men can also be victims, only acknowledging “women” as victims. This provision states that attempting to monitor a woman’s use of the internet, email, or any other electronic communication device is prohibited. The term for this activity is “cyberstalking.” It is obvious that it focuses only on women. It’s the laws that discriminate against women. Secondly, the lawmakers have not mentioned the “means of monitoring.” Even if someone behaves unintentionally, they could still be considered a stalker.

Second, the IPC’s Section 292 defines “obscenity.” Cyberstalking is defined as sending sexual materials to a victim via email, texting, social networking sites, or other channels. As to the Indian Penal Code’s Section 292, sending pornographic material over the internet with the intention of depraving the victim in the hopes that the victim will read, see, or hear it is considered an offence by the stalker.

Thirdly, Section 507 of the IPC includes “criminal intimidation via anonymous communication.” This clause states that it is unlawful for a stalker to attempt to hide his identity from the victim and keep them in the dark about the source of the threat. Thus, it ensures anonymity, which is a necessary component of cyberstalking. This clause will find the stalker guilty if they attempt to conceal their identity.

Fourthly, Section 509 of IPC relates to modesty of women reads as follows:

“Any statement, gesture, or action meant to belittle a woman’s modesty. Anyone who utters a remark, makes a sound or gesture, or displays an object with the intention of offending a woman’s modesty and hoping that the woman will hear it, see it, or feel that it invades her privacy will be punished...”<sup>1</sup>

A stalker may be reported under this provision if their actions interfere with the woman’s right to privacy by any gestures they make or by saying things in emails, messages, or on social media. He will be guilty of an offence under Section 509 of the Indian Penal Code if he engages in any such actions.

There are many issues with Section 509. Among them are the following: it is a provision that is discriminatory

against women because it only highlights a woman's modesty, despite the fact that males can also become victims of cyberstalking, which is a crime that affects people of all genders. This section requires that the words, sound, or gesture be spoken, heard, or seen, respectively. Because sound, gesture, and words cannot be heard or spoken online, cyberstalkers can easily evade the punishment detailed in this section. Lastly, it is not possible to conclude that the woman's modesty is being disparaged based on remarks seen online.

Fifth, Section 292 of the Indian Penal Code is duplicated in Section 67 of the Information Technology Act, 2000. Publication of pornographic material in "electronic form" is the subject of this section. Therefore, internet stalking is included in this area. According to Section 67 of the IT Act, a stalker is guilty of an offence if he attempts to disclose any pornographic information about the victim on social media or in electronic form with the intention of intimidating the victim.

Sixth, a portion of the offence of cyberstalking is covered by Section 67A of the Information Technology Act of 2000. This section was inserted following the 2008 amendment. It declares that a stalker will be found guilty of an offence under Section 67A of the IT Act and will face the appropriate penalties if he seeks to disseminate any "sexually explicit" material in electronic form, such as through emails, texts, or social media.

Seventhly, a newly added section of the Information Technology Act of 2000 is Section 67B. Amendment Act of 2008 introduced a new section. This section focuses on instances where stalkers target minors under the age of eighteen and disseminate images of youngsters having sex with the intention of frightening the minors.<sup>2</sup>

The stalker may breach the victim's account and post private images of the victim on social networking sites in an attempt to induce anxiety and depression in the victim's mind. It would be prohibited to publish or take pictures of someone else's private behaviour without that person's authorization, as stated in the two aforementioned provisions. However, because Section 66E refers to the victim as "any individual," it is more inclusive than Section 345C, which exhibits some gender discrimination. Section 354C requires that the victim be a "woman."

The penalties under the IT Act are significantly harsher, even though all offline rules also apply to digital media. This is important. In fact, it is important to recognise that the IT Act places a strong emphasis on the bodies and sexualities of women: Section 66A of the Act addresses a broad category of "offensive messages."

The Cyber Stalking issue and the defamatory or threatening communications conveyed by the stalker through SMS, phone calls, emails, or blogs published under the victim's name are not specifically covered by the Information Technology Act, 2000, or the Indian Penal Code, 1860. While there is no specific law that addresses this particular offence, the perpetrator may be punished under some of the provisions of the aforementioned Acts. This crime is incredibly simple to do, yet the consequences are severe and long-lasting. Both the victim's physical and emotional health may be severely impacted.<sup>3</sup>

## **Constitutional Framework and Enforcement Problem**

The main issue of territorial jurisdiction is not sufficiently addressed by either the Information Technology Act of 2000 or the Information Technology Amendment Act of 2008. In addition to other sections where the topic of jurisdiction has been raised, Sections 46, 48, 57, and 61 address the adjudication process and the appellate procedure. More details regarding police officers' rights to search and enter public areas in relation to cybercrimes and other occurrences can be found in Section 80. Cybercrimes are crimes committed using computers, and if someone hacks into an email account belonging to someone who lives in another state or country, it might be difficult to determine which P.S. should be held liable for an offence.

The solution to the problem might lie in the extradition agreement between the two nations. The offender will be sent back to the country where the crime was committed if there is an extradition agreement in existence between the two concerned nations. Therefore, if there is an agreement between the victim's country and the stalker's country, there won't be any enforcement concerns in the case of cyberstalking as well.

The primary issue that emerges is when the laws of two different nations clash. There may be instances where a stalker's actions are punishable in one nation but are not considered crimes in another. We refer to this as a Jurisdictional Issue. The issue of enforcement also surfaces in these situations. Cooperation between the two nations is necessary under this circumstance. This is the point at which extradition laws are relevant.

The Information Technology Act's Section 75 confers "extraterritorial jurisdiction" over India. This clause makes it clear that even if a criminal is not an Indian citizen, they will still be bound by the Information Technology Act's standards whether their crimes were committed inside or outside of India. as long as the offence is connected to Indian computer networks or systems. Indian laws therefore only partially solve the enforcement issue.

One of the features of cyber stalking is anonymous identity of the stalker. There has been a suggestion to put restrictions on keeping the identity anonymous. This, however, appeared to be a debatable topic as almost the laws of every country ensure Freedom of Speech and putting restrictions on anonymous identity would be violative of this freedom. In the cases of *In Re Ramlila Maidan Incident v. Home Secretary*<sup>4</sup> and *Sahara India Real Estate Corp. Ltd. v. Securities & Exchange Board of India*<sup>5</sup> the court held that the freedom of speech and expression as provided under Article 19(1)(a) is not an absolute right.

## CONCLUSION

The introduction of the internet and the ensuing developments in communication have led to a marked rise in the number of crimes related to the internet, as well as an increase in the complexity of these crimes. The legal framework pertaining to cybercrimes is not exhaustive. Many provisions are regularly enforced through amendments. Before the Information Technology Act of 2000 was developed, the fight against cybercrimes was totally undefined. Since the changes, though, it has been used honourably to provide victims of cybercrimes such cyberstalking with all of the legal remedies. Thus, people believe that as these computer networks expand, strict regulations governing behaviour on the internet will likewise be implemented, transforming the internet.

Notwithstanding, people ought to exercise prudence and self-awareness when sharing private information online. Watch what they do, and don't give any personal information to strangers. However, proper laws addressing the avoidance of cyberstalking need to be drafted. Legal provisions must be taken into account while putting preventative measures into action.

It is quite true to say that the only way to change the current situation is to replace the antiquated method of treating it with a new, effective model. The term "cyberstalking" is quite recent. The legislators and courts have been increasingly cognizant of it recently. It has been felt in many circumstances that effective legislation is required since it becomes very challenging for the enforcement agency to handle such cases. It has been demonstrated that cyberstalking is a serious offence. Both the victim's mental and physical well-being are severely damaged.

## FOOTNOTES

1. Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.
2. Information Technology Act, 2000, No. 21, Act of Parliament, 2000.
3. Vijay Mukhi and Karan Gokani, Observations on the Proposed Amendments to the IT Act 2000.
4. *Suo Motu Writ Petition (Crl.) No. 122 of 2011*, decided on Feb. 23, 2012.
5. *Media Guidelines Case, C.A. No. 9813 of 2011*, decided on Sept. 11, 2012.

\*\*\*\*\*