



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBERSTALKING IN INDIA: A COMPREHENSIVE STUDY

When someone uses electronic communication, social media and other technology to harm, harass any person, such person is said to have committed cybercrime. Cyberstalking is one of the forms of cybercrime and defined as use of the internet (email, direct messages or other means) to harass, scare or threaten someone with physical harm.¹ It may include false accusations, defamation (slander and libel), monitoring, identity theft, vandalism, doxing or blackmail.²

Reasons for cyberstalking:³

- i. Jealousy
- ii. Obsession
- iii. Revenge
- iv. Erotomania
- v. Sexual Harassment

Types of Stalking:⁴

- i. Email Stalking
- ii. Internet Stalking
- iii. Computer Stalking.

Kinds of Cyberstalkers:

¹ Clare Stouffer, *Cyberstalking: Know the signs and protect yourself*, NORTON, (Jan 23, 10:20 a.m.) <https://us.norton.com/blog/how-to/what-is-cyberstalking#:~:text=Cyberstalking%20is%20when%20someone%20uses,threaten%20someone%20with%20physical%20harm.>

² WIKIPEDIA, <https://en.wikipedia.org/wiki/Cyberstalking>, (Last visited on Jan 23, 2023)

³ Vanya Verma, *The Virtual Reality of Cyberstalking in India*, IPLEADERS, (Jan 26, 09:44 a.m.)

<https://blog.ipleaders.in/virtual-reality-cyberstalking-india/>

⁴ *Ibid.*

- i. Vindictive Cyberstalkers
- ii. Composed Cyberstalkers
- iii. Intimate Cyberstalkers
- iv. Collective Cyberstalkers

Legal provision:

The concept of ‘Cyberstalking’ traces its roots from the Indian Penal Code, 1860 and the Information Technology Act, 2000, though both the acts do not contain any specific provision for helping the victims but kind of related provision for the temporary help of the victims. Such provisions are:-

Section 354D of the Indian Penal Code, 1860 (as amended in the year 2013) provides that when any man follows a woman or attempts to follow even after disinterest shown by the woman or monitors the use of web-based activity of the woman, such person is said to commit the offence of stalking. Punishment for the same is divided into two parts.

Punishment for first conviction is 3 years and fine and subsequent conviction, 5 years and fine.

Section 354C of the Indian Penal Code, 1860 (as amended in the year 2013) defines the term “voyeurism”. Voyeurism is a form of cyberstalking.⁵ When the stalker hacks the computer of the victim to watch or capture the private photos of the victim without knowledge, said to commit the offence under this section. This is also related to Section 66E of the Information Technology Act, 2000 (as amended in the year 2008).

Section 509 of the Indian Penal Code, 1860 can also be related to cyberstalking. If the stalker through the internet or any electronic medium uses any word, gesture to insult the modesty of the woman or violate the privacy of the victim, can be made liable under this section.

Section 67 of the Information Technology Act, 2000 provides punishment for publishing or transmitting obscene material in electronic form.⁶ If the stalker publishes or transmits or attempts to publish or transmit any obscene material in electronic form about the victim so as to injure the reputation of the victim or to corrupt the victim’s image before the audience, is liable to commit offence under this section. Punishment on first conviction is 3 years and fine

⁵ Arushi Sharma, *Criminology of cyberstalking: Laws in India and UK*, 4 IJLLR 1, 12-13 (2022)

⁶ VAKUL SHARMA, INFORMATION TECHNOLOGY (LAW AND PRACTICE) 226 (Lexis Nexis 2022)

(Rs. 5 lakhs) and on subsequent conviction is 5 years (Rs. 10 lakhs). This provision is related with Section 292 of the Indian Penal Code, 1860, which defines the term ‘obscenity’.

Section 67A of the Information Technology Act, 2000 (as amended in the year 2008) is also related the offence of cyberstalking. This section incorporates the term “sexually explicit” material. If the stalker publishes or transmits any “sexually explicit” material in electronic form to the victim, he is liable under this section.

Judicial Decisions:

The case of *State (Cyber Cell) v. Yogesh Pandurang Prabhu* (2009), was highlighted because this was the first case where conviction was made under the Information Technology Act, 2000. In this case, conviction was made by relying on a crucial witness and evidence was a laptop used for the crime.⁷ The convict was punished under Section 66E of the Information Technology Act, 2000 (as amended in the year 2008) i.e., punishment for violation of privacy and section 509 of the Indian Penal Code, 1860 i.e., punishment for use of words or gesture to outrage the modesty of the woman.

Manish Kataria v. State of Punjab (2001), which emphasized the stalking of a lady Ritu Kohli, was the first documented case of cyberstalking in India.⁸ In this case the victim proclaimed that someone was maligning her identity by communicating in a vulgar language at a certain website. Since during that time, publication of obscene material was not recognized as a crime so, he was punished under Section 509 of the Indian Penal code, 1860. But the problem which arose is that Section 509 does not specifically deals with the offence of “cyberstalking”.

The case of *Prajwala v. Union of India* (2018), [ongoing case] has demonstrated that the issues related to publication or transmission of obscene information in electronic form has to be also looked from the perspective of ‘extra-territorial’ jurisdiction and Internet Technologies, keeping in view that ‘obscenity’ is no longer a local and static phenomenon. It has always been global and dynamic in nature and thus needs coordination among various stakeholders as well as strict interpretation of the statute.⁹

⁷ Pratham Gupta, *What is Cyberstalking? What are its perspectives in India?* LAW INSIDER (Jan 26, 2023, 21.05 p.m.) <https://www.lawinsider.in/columns/what-is-cyber-stalking-what-are-its-perspectives-in-india>

⁸ *Ibid.*

⁹ VAKUL SHARMA, INFORMATION TECHNOLOGY (LAW AND PRACTICE) 226 (Lexis Nexis 2022).

Stalking directly infringe a person's right to privacy guaranteed under Article 21 of the Constitution of India which provides right to life and personal liberty. This was highlighted in the landmark case of *Justice K.S. Puttaswamy v. Union of India*, AIR 2018 SC (SUPP) 1841.

Conclusion:

Stalking cases have risen nearly 97% from the year 2014 as available as per the report of National Crime Records Bureau (NCRB), 2021. Approximately 25 cases are reported every day of stalking.¹⁰ This data shows that its high time that we focus on the issue of bringing a specific statute dealing with cyber crimes in its strict sense. We have legislations but there is no specific legislation or guidelines regarding cyberstalking. We have few provisions concerning cyber crime under the Indian Penal Code, 1860 and the Information Technology Act, 2000 but they are not enough to tackle the grave offence of cyberstalking (because the laws are not specifically dealing with this offence and are more territorial in nature). Now cyberstalking also involve the perpetrators from other countries, which is difficult to control as we do not have extra territorial jurisdiction.¹¹ Therefore, there is an urgent need for global legislations for handling cyberstalking.

¹⁰ CNBC, <https://www.cnbcv18.com/india/ncrb-data-india-reported-nearly-25-cases-of-stalking-in-a-day-in-2021-still-the-numbers-may-be-way-far-from-the-reality-14660061.htm> (last visited Jan 27, 2023)

¹¹ Alok Misra, Cyber Staking: A Challenge for Web Security, RESEARCH GATE (June 03, 2020), https://www.researchgate.net/publication/315573762_Cyber_Stalking