CYBERSTALKING - A FELONY TO THE SOCIETY

Reshma Ranjith, Assistant Professor, School of Law for Women, Dhanalakshmi Srinivasan University, Perambalur

Agnes Amala Anitha T, Assistant Professor, School of Law for Women, Dhanalakshmi Srinivasan University, Perambalur

ABSTRACT

Cyberstalking, which takes the form of continuous monitoring, harassment, or intimidation via online communication platforms including social media, email, and messaging services, has emerged as one of the most urgent issues of the digital age. Important questions about safety, dignity, and privacy are brought up by the occurrence, especially for woman and children. The Indian Penal Code, 1860, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and the Protection of Children from Sexual Offences Act, 2012 are all part of the country's multifaceted legal system that addresses cyberstalking. The Criminal Law (Amendment) Act of 2013 introduced Section 354D of the IPC, which made stalking – including the monitoring of electronic communications – specifically illegal. In order to maintain consistency and clarity in the recognition of cyberstalking as a criminal offence, this clause has been kept in Section 74 of the BNS. By making identity theft, impersonation, privacy violations, and the transfer of pornographic or sexually explicit content illegal – actions frequently linked to cyberstalking – the IT Act enhances these broad rules. The POCSO Act, which forbids the use of minors in online pornography and criminalizes sexual harassment, offers more robust protections for cases involving minors. Although India has created a thorough legal framework to combat cyberstalking, this paper contends that in order to provide adequate protection in the digital realm, obstacles related to victim awareness, enforcement, and technical adaptability must be addressed.

INTRODUCTION

Internet and virtual world has become a part of our daily life. Nevelsteen describes virtual world as, "a simulated environment where many agents can virtually interact with each other, act and react to things, phenomena and the environment; agents can be zero or many human(s), each represented by many entities called a virtual self (an avatar), or many software agents; all action/reaction/interaction must happen in a real-time shared spatiotemporal non pausable virtual environment; the environment may consist of many data spaces, but the collection of data spaces should constitute a shared data space, one persistent shard."[1] Due to technology, at present in this cyber world, today's generation is facing a lot of cybercrimes, which are increasing day by day. When a person uses a computer or any other electronic device as a tool or target for committing a crime, it is termed as cyber crime. Cyber crimes includes the illegal computer-related activities like computer hacking, software piracy, cyber stalking, password breaking, child abuse, internet paedophilia, e-mail bombing, spamming, credit card fraud, theft of communication services, industrial espionage, dissemination of pornographic and sexy offensive material in cyber-space, electronic ,money laundering and tax evasion, electronic vandalism, terrorism and extortion, tele-marketing frauds, illegal interception of tele-communication[2] etc. This paper discuss cyber stalking, which is a threat to the society as it is having social, political, economical and legal effects in this century. The study also points on the concept and consequences of the crime, whether the laws which are available now are sufficient and effective to prevent cyber stalking and also the punishment and remedy for cyber stalking.

CONCEPT OF CYBERSTALKING

Stalking is a continuous process to make someone feel that they are not safe or to make a person think that they are being followed by someone or they are being aimed by an anonymous person. Cyber stalking can be represented as a new form of behaviour where the technology is used to harass one or more individuals. Cyber stalking can be defined as, "a group of behaviours in which an individual, group of individuals or organization, uses information and communications technology to harass another individual, group of individuals or organization. Such behaviours may include, but are not limited to, the transmission of threats

[1] Kim JL Nevelsteen, Virtual World, Defined From A Technical Perspective, And Applied To Video Games, Mixed Reality And The Metaverse, (John Willey & Sons, Ltd. 2018)
[2] Dr. N. V. Paranjape, Criminology & Penology With Victimology, 146 (Central Law Publications 15th ed. 2012)

and false accusations, damage to data or equipment, identity theft, computer monitoring, the solicitation of minors for sexual purposes and any form of aggression. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress."[3]

Cyber stalking has been originated in the early 21st century in America, and California was the first state to enact cyber stalking laws. This is a form of mental assault, in which the executioner frequently, unwontedly and disorderly breaks into the life of the target, with whom he no longer has a relationship, but with an intention that can be directly or indirectly detectable to the affective sphere.[4] Cyber stalking is an instance of how finest things in life may be used by some troublesome persons in the practicable manner. Internet has made it possible to communicate through electronic mails, e-chatting or instant messaging.[5]

- **Components of Cyber stalking**

  1. False Accusations

  False accusations are made by the perpetrator in order to make disgrace to the fame of a person. It can be defined as a claim or allegation which is untrue or not supportive to the actual facts.[6]

  2. Cyber Defamation

  Cyber defamation is a new concept that virtually defames a person through new medium i.e., defaming the individual's identity with the help of computer or any electronic device. If any person posts or publishes some false statement about another person through e-mail or any other platform, the individual who made the statement with an intention to defame the other would amount to cyber defamation.[7]

  3. Monitoring

  It means checking or observing a person, his behaviour, his daily activities etc in

[3] Paul Bocij, Victims of Cyber stalking: An Exploratory Study of Harassment Perpetrated via the Internet, 8 First Monday, 1 (2003)
[4] Lamber Royakkers, The Dutch Approach to Stalking Laws, 2 Cal. Crim. L. Rev. 1 (Oct 2000) https://www.boalt.org/CCLR/v3/v3royakkersnf.htm
[5] DR. J. P. MISHRA, AN INTRODUCTION TO CYBER LAW, 189, Central Law Publications, 2nd ed. 2014
[6] USLEGAL, https://definitions.uslegal.com/a/accusation/ (last visited August 12, 2025)
[7] LAWLEX.ORG, https://lawlex.org/lex-pedia/what-is-cyber-defamation/25167 (last visited August 12, 2025)

order to know their whereabouts.

4. Identity Theft

The term identity theft refers to fraud or deceit that concerns or involves stealing money or pretending to be someone to get benefits. The person whose identity is used will suffer numerous consequences when they are affected by the evildoer's activity.[8]

5. Cyber Threats

Cyber threat can be defined as a malicious act that pursue to damage information, steal data, or interrupt the digital life of a person or anything in general. It can be considered as cyber-attacks which involves computer viruses, data breach and Denial of Service (DoS) attacks.[9]

6. Cyber Vandalism

Vandalism simply means purposefully destroying or damaging another person's property. Cyber vandalism means destroying or damaging the data or information when the network service is terminated or obstructed. It includes any kind of tangible damage done to the computer or any electronic device of such person. Vandalism can take place in the form of theft of a computer, some part of a computer or a peripheral attached to the computer.[10]

7. Solicitation for Sex

Solicitation means an earnest request. In cyber world, internet solicitation includes seeking or arranging services to lay out sexual indulgence over the web by interchanging something having value or with money consideration. The illicit cases that involve online solicitation can be charged as either an offence or a felony

[8] Pulkit Tare, Identity Theft, Legal Service India, 1(2018)
[9] Hugh Taylor, What are Cyber Threats and What to do about them, The Missing Report, (August 12, 2025, 3:30 PM), https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/
[10] Nidhi Narnolia, Cyber Crime in India: An Overview, Legal Service India, 3(2021)

sex crime.[11]

8. Doxing

Dox or Doxing is a web-based activity in which the troublemaker would analyse and broadcast or leak the private or personally known data of another person including name, address, photographs, phone numbers and other information. This information is collected by way of social media websites, hacking, social engineering etc. and is broadcasted without their consent. Doxing is carried out in order to blackmail or to take revenge on a person.[12]

9. Blackmail

It can be defined as an act of intimidating or pressurizing to disclose and publicize considerably correct or wrong data about a particular person or a group in exchange for demands including personal, sexual desires and monetary gain.[13]

10. Cyber Harassment

A continuous, unrequested and aggressive practise of a person by way of cyberspace with an aim to panic, discourage, embarrass, threaten or disturb another person is termed as cyber harassment.[14]

- **Reasons for Cyber stalking**

1. Fascination or Obsession

It means an attraction to the victim. The attraction may be physical or mental. This obsession can lead to stalking. These kinds of perpetrators may behave like abnormal persons.[15]

[11] David L Freidberg, Internet Solicitation, Freidberg Attorney at Law, (August 12, 2025, 3:50 PM), https://www.chicagocriminallawyer.pro/internet-solicitation.html
[12] AARAMBH INDIA, https://aarambhindia.org/knowing-risks-cyberbullying-cyberstalking-trolling-doxing/ (last visited August 12, 2025)
[13] Niharika Goel, Cyber Blackmail: Diligent Steps Towards Legal Remedy, iPleaders, (August 12, 2025, 6:15 PM), https://blog.ipleaders.in/cyber-blackmail-diligent-steps-towards-legal-remedy/
[14] VIKASPEDIA, https://vikaspedia.in/education/didital-literacy/information-security/being-safe-online-1/cyber-harassment (last visited August 12, 2025)
[15] Nirmal K Vijayan, Challenges in regulating Cyber Stalking, Legal Service India, 2(2013)

2. Jealousy, revenge and Hate

Jealousy is a kind of negative emotion which can be a reason for stalking. It happens in-between the partners or ex-partners. In some cases, the stalker does not have particular reason to take revenge on the victim, but he/she chooses such person as a medium to express their dislike and vengeance through internet.[16]

3. Erotomania

It is an uncommon psychiatric condition that occurs when a person is obsessed with the thought that another person is intensely in love or affectionate to them. The opposite person can be well-known person like a celebrity, politician etc. or a wealthy person or someone with a high-class background. Erotomania is also known as De Clerambault's syndrome.[17]

- **Consequences Of Cyber Stalking**

1. Fear
2. Anger
3. Insomnia
4. Depression
5. Anxiety
6. Post-Traumatic Stress Syndrome (PTSD)
7. Suicidal Ideation

INDIAN LAWS ON CYBER STALKING – PUNISHMENT & REMEDY

Cyber stalking is the prolonged and unwelcome use of internet communication to harass, intimidate, monitor, or threaten another person. It is a serious invasion of privacy and

[16] Vanya Verma, The Virtual Reality of Cyberstalking in India, iPleaders, (August 12, 2025, 6:50 PM), https://blog,ipleaders.in/virtual-reality-cyberstalking-india/
[17] HEALTHLINE, https://www.healthline.com/health/erotomania , (last visited August 12, 2025)

personal security that frequently leaves victims with long-term psychological, social and occasionally bodily ramifications. In India, the tremendous expansion in internet usage and broad use of social media platforms has made cyber stalking a major concern. According to data from the National Crime Records Bureau (NCRB), internet harassment and stalking have been steadily increasing in recent years. This issue is addressed in Indian law by combining general criminal law under the Indian Penal Code, 1860 (IPC) and its successor, the Bharatiya Nyaya Sanhita, 2023 (BNS), with specialized legislation such as the Information Technology Act, 2000 (IT Act) and the Protection of Children from Sexual Offences Act, 2012 (POCSO Act). These frameworks work together to form a multilayered legal environment that protects victims from internet abuse.

The Criminal Law (Amendment) Act of 2013, which included Section 354D, was the first to recognize stalking as a separate offence under IPC. This clause criminalized physical and online stalking, describing it as following a woman, seeking to contact her despite obvious disinterest, or monitoring her computer communication. The punishment prescribed was imprisonment for up to three years on the first conviction and up to five years on consecutive convictions, as well as a fine. This provision has been kept in Section 74 of the Bharatiya Nyaya Sanhita, 2023. The BNS maintains continuity with the IPC while modernizing the terminology to reflect the growing occurrence of digital harassment. Thus, both paradigms explicitly define cyberstalking as a criminal offence.

According to Section 354 of IPC, soul virtue of a woman is her gender or sex. Any action or assault that lead to trouble a woman's sense of dignity or decency is the paramount test taken in order to identify whether the humility or modesty of a woman is injured.[18] In 1995, the Supreme Court unambiguously directed the Magistrate to accept the complaints relating to sexual assault under this Section read with Section 509 in the famous case which is popularly known as "The Butt Slapping Case" where a senior IAS officer of Punjab, Mrs. Rupan Deol was slapped on her butt by the DGP of Chandigarh Police, Mr. KPS Gill in an official party where both the officers were invited. A complaint was filed under Sections 341, 342, 352, 354 and 509 of IPC by Mrs. Bajaj against Mr. Gill.[19] The court held that, "The Magistrate did not always take cognizance of the cases under sexual harassment until in the above mentioned case

[18] Rishabh Sachdeva, Introduction of Stalking into Indian Legal Regime, Soolegal (August 13, 2025, 11:00 AM), https://www.soolegal.com/roar/introduction-of-stalking-into-indian-legal-regime
[19] Vanshika Sharma, Cyber Stalking: The Crime, Indian Law Portal, (August 13, 2025, 11:50 AM), https://indianlawportal.co.in/cyber-stalking-the-crime/

Supreme Court clearly directed the magistrate to take cognizes of the complaint under Section 354 read with Section 509".[20]

A landmark judgment was made in order to take sufficient steps regarding sexual harassment of women in workplace in the case of Vishaka v. State of Rajasthan.[21] In 1999, another landmark judgment was made by the Apex court that any act that leads to sexual harassment of women in workplace is a clear-cut violation of fundamental rights.[22]

While IPC and BNS define stalking as a general offence, the Information Technology Act of 2000 expands these laws by addressing particular cyber offences that commonly overlap with cyberstalking. Section 66C punishes identity theft, a prevalent form of harassment in which criminals create phony profiles the victim's name. Section 66D sanctions cheating by impersonating someone using computer resources, whereas Section 66E targets privacy violation such as taking, publishing, or transferring photos without permission. Sections 67 and 67A also make it illegal to publish or transmit obscene and sexually explicit information electronically.

A landmark judgment was passed by Ld. Additional Chief Metropolitan Magistrate, Egmore, in State of Tamil Nadu v. Suhas Katti.[23] This case is considered as the first case to provide conviction under the Information Technology Act, 2000. In this case, the perpetrator was charged and convicted with Section 67 of IT Act along with Section 469 and 509 of IPC since the accused has misused the identity of the victim to send obscene message that amount to cyberstalking and e-mail spoofing under this Act.[24]

The first cyberstalking case in India was reported in 2001. The victim has been stalked by the accused by using her identity and sending obscene content to the public. The accused also distributed her address and contact to the people. Later the victim started getting nasty i.e., obnoxious message from people. The case was charged under Section 509 of IPC but after the Information Technology (Amendment) Act, 2008, Section 66A was inserted and the accused

[20] Rupan Deol Bajaj v. Kanwar Pal Singh Gill, 1995 SCC (6) 194
[21] Vishaka & Ors. v. State of Rajasthan & Ors., AIR 1997 SC 3011
[22] Apparel export Promotion Council v. A. K. Chopra, AIR 1999 SC 62
[23] State of Tamil Nadu v. Suhas Katti, C. C. No. 4680/2004
[24] Pritham Banerjee & dr. Pradip Banerjee, Analysing the Crime of Cyberstalking as a threat for Privacy Right in India, 7 JCIL 35, 44 (2022), https://icjl.lsyndicate.com/wp-content/uploads/2022/02/Analysing-the-crime-of-Cyberstalking-as-a-threat-for-privacy-right-in-India.pdf

was charged according to the new law.[25]

A complete definition for cyber stalking was given in the case, State (Cyber Cell) v. Yogesh Pandurang Prabhu – "Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a website or a discussion group. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected."[26]

When the victim is under the age of 18, special safeguards are provided. The Protection of Children from Sexual Offences Act of 2012 (POCSO Act) includes internet harassment and cyberstalking against minors under the age of eighteen. Sexual harassment is defined in Section 11 of the Act as repeated following, contacting, or making sexually coloured remarks, whether offline or online, and Section 12 provides for up to three years in prison for such conduct. Sections 13-15 of the act penalize the use of children in pornographic content, which is increasingly being created, stored, and disseminated via internet platforms. As a result, when cyberstalking involves a child victim, measures from both the BNS and the POCSO Act work together to ensure enhanced protection and child friendly procedures throughout investigation and trial process.

PLATFORMS FOR REPORTING CYBER STALKING

- **Cyber cell**

  Cyber cell is a part of criminal investigation department that functions and deals with those crimes related to the cyber space. If there is no Cyber cell unit in the jurisdiction where the offence happens, the victim can file a complaint to the local Police Station, or to the Commissioner of Police or to the Judicial Magistrate of that city.[27]

- **National Cybercrime Reporting Portal**

  A person or a victim can report the crime through this online portal and the authorised police officers would take charge of the crime. In most of the cybercrimes, the victims

[25] Manish Kathuria v. Ritu Kohli, C. C. No. 1616/2014
[26] State (Cyber Cell) v. Yogesh Pandurang Prabhu, C. C. No. 3700686/PS/2009
[27] Anubhav Pandey, Law Punishing Cyber Stalking and Online Harassment, iPleaders, (August 16, 2025, 8:30 PM), https://blog.iplears.in/cyber-stalking/

hesitate to register complaint directly to the police station therefore online portals are helpful.

- **National Commission for Women**

  It is an Indian Government statutory body that deals with matters concerning women. One can register a complaint to online Grievance Redressal Cell which functions under this commission.

- **CERT-IN**

  CERT-IN means Indian Computer Emergency Response Team that works under Ministry of Electronics and Information Technology. It is national nodal agency designation by the Information Technology (Amendment) Act, 2008 in order to stop the cases related to computer security threats. CERT provides e-form, in which the details of the cyber crime can be submitted.[28]

- **Report to Websites**

  In most of the social media websites, a reporting mechanism is provided for the account users. These websites are obliged the IT (Intermediary Guidelines) Rules, 2011 to act within 36 hours to disable information relating to the offending content.[29]

CONCLUSION

The Indian legal framework provides a multifaceted and comprehensive strategy to combating cyberstalking. The IPC established the groundwork by making stalking a criminal offence, which is now protected under the BNS. The IT Act improves the framework by criminalizing identity theft, privacy violations, and obscene content on the internet, while the POCSO Act strengthens protection for children. When taken as a whole, these rules make cyberstalking a crime and give victims several options. However, as legal recognition must be translated into actual protection in the digital era, the efficacy of these rules ultimately rests on strict enforcement, prompt investigation, and broad awareness.

[28] Id
[29] H2S MEDIA, https://www.how2shout.com/newa/cyberstalking-and-its-legal-remedies-in-india.html , (last visited August 16, 2025)