Cyberstalking Against Women in the Indian Perspective: An Overview

¹Priya Gupta, ²Dr. Abhay Chand Mall Visen

¹Research Scholar, Department of Law, Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur, U.P. ²Assistant Professor, Department of Law, Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur, U.P.

Abstract:

In India, women have got the status of goddess since ancient times. Crimes are being committed against women from ancient times to present day, but in the present times there has been an increase in crimes against women, which were earlier crimes against women in the physical world. But today in the age of information and technology, the same crimes against women have started happening in the cyber world as well. The present existing laws for Cyber stalking like The Information Technology Act 2000, Indian Penal Code 1860 and other laws are not able to deal with it completely, so today there is a need for strict and strong laws to deal with this crime. This research paper specifically focuses on studying the crime of cyber stalking against women in India with a legal point of view.

Key words: Cyber crime, Cyberstalking, Victims of Cyberstalking, Online crimes against women, Online crimes, Cyberstalkers.

I. INTRODUCTION

Cyberstalking is a type of crime. In the cyberstalking there is an involvement of two persons – Firstly, the stalker is also known as attacker who do the crime and, Secondly, the Victim who is harassed by the stalker. Cyber stalking is also known as cyber crime. This form of stalking is considered an extension of personal stalking and cyberbullying. Cyber which is related to the internet and stalking means to browsing anyone's online history with the help of any social media or in other websites to know about the particular person is term as stalking.¹ Cyberstalking defined as the use of the internet and other technologies to stalk and harass another individual. Cyberstalking can be done through a set amount of text messages, emails,

and social media posts. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, doxing, or blackmail. When it comes to cyberstalking, those who engage in this behavior use a variety of tactics and techniques to harass, humiliate, intimidate, and control their targets. In fact, many of those who engage in cyberstalking are technologically savvy as well as creative and come up with a multitude of ways to torment and harass their targets. The consequence of cyberstalking also impacts of person's mental health and overall wellbeing, people who have been a target or cyber stocking experience distress, anxiety and depression. There are even reports that targets of cyberstalking may experience post traumatic stress disorder and suicidal ideation. In early 1990s, stalking activities was more concentrated with celebrities by their fans and called as 'Star-Stalking'. Nowadays, the general criminal activity is no longer limited within the material world rather it has expanded to the virtual world as well. In this digital era, cyber space has given rise to unprecedented changes in the daily activities of human life. Information and Communication Technology (ICT) which was initiated for general welfare, betterment of people's lifestyle and comfort, gradually has become a weapon to criminal aspirations. Anonymity, Authority and Attention which not only attracts the criminal minded people, rather it also provides an opportunity for common people to unleash their negative side to obtain pleasure in dark fun. Generally, aims of these stalkers is to enter in the private space of their target. Incidentally, cyber stalkers always try to monitor each and every move of their target by way of repeated e-mails, messages, annoying phone calls or in any other mode. However, the right to privacy being an international human right has been well recognized by the Universal Declaration of Human Rights (UDHR) since 1948 as well as under the International Covenant on Civil and Political Rights (ICCPR) since 1966. Later on, the Supreme Court of India has clearly affirmed that Right to Privacy is very much a part of the fundamental right guaranteed under Article 21 of the Indian Constitution. Herewith, the apex court further noted, "privacy is not lost or surrendered merely because the individual is in a public place.

Privacy attaches to the person since it is an essential facet of the dignity of the human being." So, this cyberstalking behavior not only causes distress and a sense of threat in the mind of victim but violate fundamental

¹ available at: https://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html

human rights to privacy, dignity and personal liberty of the victim. It is pertinent to mention that a report made by WHOA in 2013 found that - (i) the majority of cyberstalking victims are between 18 to 29 years of age; (ii) roughly 40 percent of cyber stalkers are male; (iii) approx. 60 percent cyberstalking victims are female. Notably, Harold D'Costa, the director of Cyber Intelligent firm and cop trainer states, "We are getting nearly two hundred such (cyber-crime) cases every day from all over Maharashtra. India is the second largest user of Internet in the World, while Maharashtra is the largest internet user in the country. Nearly 16.04 crore Indians are registered on various social networking sites- that really makes it tough to catch these stalkers." Further, this crime of cyberstalking was geared up during the covid-19 lockdown period when people were compelled to spend most of the time within the cyber world.²

MEANING: Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organisation.³

DEFINITION:

• Oxford Dictionary

Cyberstalking is the act of harassing someone using online or mobile communication tools.

• Merriam-Webster Dictionary

The use of electronic communication to harass or threaten someone with physical harm

Collins dictionary

Cyberstalking is the use of the internet to contact someone or find out information about them in a way that is annoying or frightening.

• According to Wikipedia

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.⁴

TYPES (KINDS):

1. Specific Motivation and Reasoning

Can come in many forms with each presenting its own specific motivation and reasoning. Regardless of the motivation and reasoning, all forms of cyberstalking serve the purpose of harassing and remaining in contact with their chosen victim to either fulfill a fantasy or complete a goal:

1) **Cyberstalking by strangers**: Victims of cyberstalks whose perpetrators were strangers would have met the perpetrator in an online platform like Facebook or Instagram. Due to the interaction starting completely online, the perpetrator will groom their victims to build trust so the victim will be willing to meet in person.

2) **Gender-based stalking**: It has been found that women disproportionately become targets of cyberstalking. Acts of cyberstalking against women can include sexually explicit messages, sextortion, and revenge pornography.

3) **Intimate partner cyberstalking**: Cyberstalking by an intimate partner has been accounted for the majority of reported stalking cases. In a study conducted by Smoker and March, women were found to be more likely to engage in cyberstalking of an intimate partner.

4) **Cyberstalking by online mobs**: This type of cyberstalking typically involves a perpetrator posting personal information, also known as doxing their victim in online forums. Due to the messaging and content, the perpetrator can be seen as encouraging or facilitating the harassment of their victim. As a result, members of the group will take part in the behavior against the victim.

2. Other types of Cyberstalking

Three Other different types of Cyberstalking can be classified into three different types, that are as follows:-

- 1) **Email stalking;**
- 2) Internet stalking;
- 3) Computer stalking.

https://en.wikipedia.org/wiki/Cyberstalking#:~:text=Cyberstalking%20is%20the%20use%20of,often%20define

d%2

0as%20unwanted%20behavior.

 ² https://jcil.lsyndicate.com > A...PDF ANALYSING THE CRIME OF CYBERSTALKING AS A THREAT ...
³ https://en.wikipedia.org/wiki/Cyberstalking

⁴

CONCEPTUAL DEVELOPMENT OF CYBERSTALKING:

Concept of 'traditional stalking' and 'cyberstalking' are closely related with each other, even so these concepts may not be used as synonymous, because cyberstalking indeed represents a new form of deviant behaviour which is efficient to distinguish it from the concept of traditional stalking. Basically, cyberstalking is partly derived from the concept of traditional nuisance where the offender makes use contemporary modern technology to commit crimes in cyber space. In traditional as well as online forms, stalkers possess behaviors and tactics with mala fide intention to harass and in some cases, it resulted in threat or intimidation against victim. Like traditional stalking, cyberstalking is also fueled by rage, anger as well as desire to control and create influence over the victim and occasionally it komay further trigger by action or inaction in victim's part. Notably, Bociji and McFarlance defined 'cyberstalking' as "a group of behaviors by a person who uses Information and Communications Technology (ICT) to harass another person." They also provided a list of behaviors which may be termed as cyberstalking, such as (i) transmission of threats and false accusations; (ii) damage to data or equipment, identity or data theft; (iii) computer monitoring, the solicitation of minors for sexual purposes and (iv) any other form of aggression.

Further, cyberstalking based on the victim's knowledge, can be divided into two types. That is where stalking attitude is noticed or known by the victim is called as 'Overt' and when such activities of cyber stalker are hidden from the victim's knowledge is termed as 'Covert'. Thus, this modified and extended behavior of cyberstalking makes it more complex and challenging to tackle. Further, cyberstalking is not only limited with mere individual but denotes any person that includes the corporate entities as well. So, the aforesaid cyberstalking behaviors gave a diversified vulnerability over the right to privacy and prominently imposed threat against the protection of data around the cyber space. On the other hand, few unique challenges which again differentiate cyberstalking from the stalking have been enumerated as follows: (i) Geographical Proximity- Cyberstalking performed at virtual world which is not restricted by any types of territorial boundaries. Therefore, cyber stalker and victim may be or may not be locally connected with each other as there have no prior requirement of physical confrontation; (ii) Anticipation - In case of traditional stalking, it is more convenient for investigator to track concern stalker in comparison with cyberstalking. As in later situation, identity of offenders may be hidden easily behind the veil of anonymity; and (iii) Spontaneity - cyber stalkers may randomly select their victims since technology provide a shield to conceal their identity.⁵

I.INTERNATIONAL CONCERN FOR CYBERSTALKING

Cyberstalking is a criminal offense under various state anti-stalking, slander and harassment laws. That's why almost all the countries of world have law to prevent cyberstalking. From time-to-time conference has been organised globally to prevent cyberstalking. There is also international investigation organisation to deal with cyberstalking at the international level. Similarly, there are law in India to prevent cyberstalking.

II.NATIONAL PERSPECTIVE

1. LEGAL PROVISIONS:

• Information Technology Act, 2000

1) Section 66A(b) of The Information Technology Act, 2000 says that false and meant for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will; meant to deceive or mislead the recipient about the origin of such messages, etc., shall be punishable with imprisonment up to three years and with fine.

2) Section 67 of The Information Technology Act, 2000 states that when any option content material is published, transmitted or caused to be published in any electronic form, then it is a crime of obscenity punishable with imprisonment for up to 5 years with fine of up to Rs.1 lakh. A second or subsequent conviction is punishable by imprisonment for up to 10 years with a fine of up to Rs. 2 lakh.

• Bharatiya Nyaya Sanhita, 2023

The Act includes stalking as an offence under sections:

1) Section 78 of states that the punishment for stalking is imprisonment for up to three years and a fine on the first conviction. On a second or subsequent conviction, the punishment is imprisonment for up to five years and a fine.

2) Section 354 - The Bharatiya Nyaya Sanhita (BNS) 2023, Section 354 (1) Covers the offence of defamation, Section 354 (2) Describes the punishment for defamation, which includes: Simple imprisonment for up to two years, a fine or both simple imprisonment and fine

3) Section 79 of the Bharatiya Nyaya Sanhita (BNS) of 2023 is a law that protects women from actions that intend to insult their modesty. The law punishes anyone who: Uses words, makes gestures, or exhibits an object

⁵ https://jcil.lsyndicate.com > A...PDF ANALYSING THE CRIME OF CYBERSTALKING AS A THREAT ...

to insult a woman's modesty, intends for the woman to hear the words or see the object, Intrudes on a woman's privacy to offend her. The punishment for violating Section 79 is simple imprisonment for up to three years and a fine.⁶

2. JUDICIAL APPROACH:

Manish Kathuria vs. Ritu Kohli this case is the first case in India dealing with cyber stalking, in 2001 first time cyber stalking's case had been reported in India. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same. So, in 2008. Indian legislature has amended the IT Act 2000 and made provisions for cyber stalking. The IT Act, 2008 does not directly address stalking. But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in the IT Act, 2008. Hence the most used provision for regulating cyber stalking in India is Section 72 of the IT Act, 2008.⁷

*State of Tamil Nadu vs. Suhas Kutti*⁸, this case is related to obscenity posting about a divorce woman in Yahoo Messenger Group. It is the only unique case achieving conviction within short span of 7months from filing FIR. This case is a landmark case in history of Cyber Crime.Hence the accused was found guilty u/s 469,509 of IPC and 67 of IT Act. He was convicted and sentenced for rigorous imprisonment for 2 years u/s 469 IPC and also to pay a fine of Rs.4000.

State Cyber Cell vs. Yogesh Pandurang Prabhu⁹, the present case discusses sending obscene materials by email. Yogesh was accused of cyberstalking by sending obscene emails to a reporter. Court held that accused intentionally and knowingly intervened privacy of reporter which attracts Section 66E of Information Technology Act, 2000 and Section 509 of IPC. However, offence under Sections 67 and 67A of Information Technology Act, 2000 was not established beyond reasonable doubt. So, accused was convicted under Section 509 of IPC and Section 66E of Information Technology Act, 2000 was not established beyond reasonable doubt. So, accused was convicted under Section 509 of IPC and Section 66E of Information Technology Act, vide Section 248(2) of CrPC.

The Shilpa Shetty case, in 2014, Bollywood actress Shilpa Shetty filed a complaint against an unknown person who was relentlessly cyberstalking her. The person created a fake Twitter account in her name and posted derogatory and defamatory content. The Mumbai Police Cyber Cell investigated the case, and the accused was later arrested.

The Varnika Kundu case, in 2017, Varnika Kundu, a DJ in Chandigarh, was stalked by Vikas Barala, the son of a prominent politician. The incident gained significant media attention and sparked a national debate on women's safety. The accused was charged with multiple offenses, including stalking and attempted abduction.

The Nirbhaya case, while the Nirbhaya case primarily involved a brutal gang rape in 2012, it also highlighted the issue of cyberstalking. The perpetrators, before the incident, stalked and harassed the victim through phone calls and text messages. This case led to widespread outrage and resulted in significant legal reforms related to crimes against women.

The Malvika Joshi case, in 2016, a 21-year-old student named Malvika Joshi filed a complaint against a man who had been stalking her online for months. The accused, who claimed to be a software engineer, created multiple fake profiles on social media platforms and sent explicit and threatening messages to Malvika. The case shed light on the issue of cyberstalking and the need for stricter laws to combat such crimes.

⁶ https://www.google.com/search?q=section+79+in+bns&client=ms-android-motorola-

rvo3&sca_esv=3ddc15aac6af2d0d&sxsrf=ADLYWILVEEsZPzbd72Taow1MoLzXZnW8sg%3A173341058599 8&ei=Gb9RZ9fKPOOb4EPmsa22AY&oq=sec+79+in+&gs_lp=EhNtb2JpbGUtZ3dzLXdpei1zZXJwIgpzZWM gNzkgaW4gKgIIATIHEAAYgAQYCJIHEAAYgAQYAQAQHAQDYGQZGAsORqAIPwgIHECMYJxjqAsICBBAJGCfCAgoQIxiABBgnGIoFwgILEA AYgAQYkQIYigXCAgsQABiABBixAxiDAcICChAAGIAEGEMYigXCAgwQABiABBhDGIoFGArCAgUQL hiABMICChAAGIAEGBQYhwLCAgcQLhiABBgKwgIFEAAYgASYAxXxBdctvm0HMipckgcFMy4yLjigB5 JL&sclient=mobile-gws-wiz-serp

⁷ https://dullbonline.wordpress.com/2020/10/14/ritu-kohli-case

⁸ https://www.lawnn.com/judgement-tamil-nadu-vs-suhas-kutti/

⁹ https://blog.ipleaders.in/case-analysis-the-state-cyber-cell-v-yogesh-pandurang-prabhu/

Divya Sharma, in 2020, noticed that a random Instagram user liked nearly 200 of her photos. She disregarded it as harmless until he began making inappropriate remarks. "He then started sending me DMs asking if I wanted to go on a date with him, which I continued to ignore," the Pune-based Archeology student recalls. He became enraged and started abusing me, threatening to make me his wife by force." That's when Divya filed an online complaint with the cyber police, which resulted in the abuser's account being suspended and the abuser being punished. She believes that "no one has the right to threaten you in DMs or comments.¹⁰

3. PREVENTIVE MEASURES:

1) **Be cautious with personal information**: Avoid sharing sensitive personal information, such as your address, phone number, or financial details, on public platforms or with unknown individuals online. Be mindful of the information you share on social media and adjust your privacy settings to limit access to your personal data.

2) Use strong and unique passwords: Create strong, complex passwords for your online accounts and avoid using the same password for multiple accounts. Regularly update your passwords and consider using a password manager to securely store them.

3) **Be mindful of your social media presence**: Review your social media profiles and adjust privacy settings to control who can see your posts and personal information. Be cautious about accepting friend requests or connections from unknown individuals. Avoid sharing your location in real-time or posting vacation plans, as it can make you more vulnerable to stalking.

4) **Secure your devices and accounts**: Keep your devices, including computers and smartphones, updated with the latest security patches and antivirus software. Enable two-factor authentication (2FA) for your online accounts whenever possible to add an extra layer of security.

5) **Be vigilant of phishing attempts**: Be cautious of suspicious emails, messages, or links from unknown sources. Cyberstalkers may use phishing techniques to trick you into revealing personal information or gaining access to your accounts. Avoid clicking on suspicious links and verify the authenticity of emails or messages before responding.

6) **Report and block**: If you experience cyberstalking or harassment online, report the incident to the relevant platform or website. Most social media platforms have reporting mechanisms in place. Additionally, consider blocking the individual responsible for the harassment to limit their access to your online presence.

7) **Maintain a record:** Keep a record of any harassing or threatening messages, posts, or emails you receive. Take screenshots or save copies as evidence, as this information can be useful if you decide to report the cyberstalking incident to the authorities.

8) **Stay informed**: Keep yourself updated about the latest cybersecurity practices and online safety tips. Educate yourself about the risks and potential threats associated with online interactions and share this knowledge with family and friends.

4. NCRB REPORT:

According to the National Crime Records Bureau's most current data Maharashtra has reported the most cases of cyberstalking/bullying of women for the third year in a row, with 1,126. Maharashtra also accounted for one-third of the 2,051 cyber stalking/bullying cases reported in India between 2020 and 2023. With 184 cases, Andhra Pradesh came in second, followed by Haryana with 97. Maharashtra ranked second among states in terms of cybercrime against women, with 1,503 cases registered in 2022 versus 1,262 in 2020, representing a 19% rise. Karnataka topped the list, with a 509% increase in instances (2,698 in 2023 compared 1,374 in 2022). In Maharashtra, the conviction rate for cybercrime has been exceptionally low in the recent three years, with only 56 of the 4,500 plus detained offenders being imprisoned.¹¹

III.FINDINGS

The paper finds differences in legal terminology as a major difficulty in combating cyber stalking. Lack of clarity in defining cyber stalking may result in variations in identifying and prosecuting offenders. The findings suggest that jurisdictional difficulties prevent effective enforcement of cyber stalking laws. The worldwide nature of the internet hampers investigations and coordination among law enforcement organisations, especially in situations involving criminals and victims from different jurisdictions. According to the study, victim reluctance, fear of reprisal, and a lack of information about possible legal remedies all contribute to underreporting of cyber stalking cases. Underreporting undermines effective intervention and enforcement initiatives. Law enforcement

¹¹https://www.google.com/search?q=cyberstalking+report+of+ncrb&oq=cyberstalking+report+of+ncrb&gs_lcrp =EgZjaHJvbWUyBggAEEUYOTIJCAEQIRgKGKABMgkIAhAhGAoYoAEyBwgDECEYjwIyBwgEECEYjw LSAQYtMWowajmoAgCwAgE&client=ms-android-motorola-rvo3&sourceid=chrome-mobile&ie=UTF-8&chrome_dse_attribution=1

organisations confront resource constraints, such as limited technology capabilities, specialised training, and dedicated people, which hinder their capacity to properly investigate and respond to cyber stalking crimes. Victim assistance mechanisms include shortcomings, such as difficulties accessing support services, getting measures of protection, and navigating the system of law. Insufficient victim support exacerbates the pain and harm suffered by victims of cyber stalking.

IV.CONCLUSION AND SUGGESTIONS

Cyberstalking is a serious crime, to deal with which there is a need to make strict laws by amending the IT Act, 2000. There is a need to create separate cell for the investigation. And a separate law needs to be made. Special training must be given be the officers to deal with the Cyberstalking against women. And the judiciary of India will have to make an important contribution to stop the Cyberstalking against women happening in India.

REFERENCES

- Debarati Halder, K. Jaishankar, Cyber Crime Against Women in India, 1st Edition, 2017. [1].
- [2]. Debarati Halder and K. Jaishankar, Cyber Crime and Victimization of Women Laws, Rights And Regulations, 2012.
- [3]. V. Nandan Kamath, Law relating to Computers, Internet and E- commerce: A Guide to Cyber Laws and the Information Technology
- Act, 2000 [4]. Dr. Pawan Duggal, Text Book on Cyber Law
- Dr. Karnika Seth, Cyber Crime Against Women: An Indian Law Perspective, 2018 Edition. [5].
- https://www.legalserviceindia.com/legal/articl e-1048-cyber-stalking-in-india.html [6].
- [7]. https://jcil.lsyndicate.com > A...PDF ANALYSING THE CRIME OF CYBERSTALKING AS A THREAT ...
- [8]. https://en.wikipedia.org/wiki/Cyberstalking
- [9]. https://en.wikipedia.org/wiki/Cyberstalking#:~:text=Cyberstalking%20is%20the%20use%20of,often%20defined%20as%20unwant ed%20behavior.
- [10]. https://dullbonline.wordpress.com/2020/10/14/ritu-kohli-case
- [11].
- https://www.legalserviceindia.com > ...Cyber stalking in India Legal Service India https://jcil.lsyndicate.com > A...PDF ANALYSING THE CRIME OF CYBERSTALKING AS A THREAT ... [12].
- [13]. https://www.google.com/search?q=cyberstalking+report+of+ncrb&oq=cyberstalking+report+of+ncrb&gs_lcrp=EgZjaHJvbWUyBg gAEEUYOTIJCAEQIRgKGKABMgkIAhAhGAoYoAEyBwgDECEYjwIyBwgEECEYjwLSAQYtMWowajmoAgCwAgE&client= ms-android-motorola-rvo3&sourceid=chrome-mobile&ie=UTF-8&chrome dse attribution=1
- [14]. https://salahmashvara.co.in/cyber-stalking-cases-in-india/