International Journal of Research in Social Sciences
Vol. 15 Issue 04, April 2025,
ISSN: 2249-2496 Impact Factor: 7.081 UGC Approved
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

"Stalking" as a crime with special quotation to "Cyber Crime" in India Stalking itself includes bullying, harassment, intimidation, defamation and thus victimization.

ANANYA CHAKRABORTY

Lecturer, Karimganj Law College

Abstract

Stalking is characterized by a pattern of unwanted and repeated behaviors that cause a target to experience fear, distress, or other forms of harm. These behaviors can include physical surveillance, harassment, threats, and even physical harm. The motives behind stalking can vary, ranging from a desire for a relationship to a delusional belief in romantic destiny. Stalking is generally defined as a unwanted, and intrusive behaviors directed towards a specific person, causing them to feel fear, harassment, or intimidation. These behaviors can include physically following someone, monitoring their online activity, sending unwanted messages or gifts, or even damaging their property. Stalkers may have a range of motivations, including a desire for a romantic relationship, a feeling of being rejected or humiliated, or even a delusional belief that they have a special connection with the victim. Stalking can have severe and lasting impacts on victims, including anxiety, depression, and fear for their safety. Stalking is a crime in most jurisdictions, and perpetrators may face legal penalties and psychological evaluations. The internet has also created new avenues for stalking, with cyber stalkers using online platforms to harass and monitor their targets. My experiments of these study draws the attention of the learners about legal awareness of this crime and also defining differences and transform awareness about laws about these cyber crimes specially of cyber stalking. I concluded my writing with a short but useful and important summary and a very much well protected steps as safeguard against cyber stalking and cyber crimes.

Introduction :- Although stalking is frequently known as simple, innocent behaviour, it can be frightening and upsetting for the victim. It is repeated and unwanted surveillance by a person or group towards another person; in a simpler sense, one can co-relate stalking to harassment and intimidation as the victim ultimately has to take the damage, relocate, change employment, and occasionally change their identity to escape the stalker.

Meaning of stalking :- The term Stalking means consistently following any particular person over a long period of time. This activity also involves the harassment or threatening behavior.

Stalking is frequently equated with harassment and torture by someone passionately after another individual. Insane narcissism, anger, rage, retaliation, envy, obsession, psychiatric illness, power and control, sadomasochistic fantasies, sexual deviance, internet addiction, or religious fanaticism are just a few of the psychological factors that lead to stalking. Other crimes, including theft, kidnapping, home invasion, extortion, trespassing, acid attacks, etc., can result from stalking.

International Journal of Research in Social Sciences
Vol. 15 Issue 04, April 2025,
ISSN: 2249-2496 Impact Factor: 7.081 UGC Approved
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Definition of stalking :-

A crime of engaging in a course of conduct directed at a person that serves no legitimate purpose and seriously alarms, annoys, or intimidates that person.

- Merriam Webster

The crime of illegally following and watching someone over a period of time.

- Cambridge Dictionary

Stalking is the willful, malicious, and repeated following or harassing of another person that threatens his or her safety.

- Melroy and Gothard

Meaning of cyber crime :-

In the cyber stalking is a use of the internet or any other electronic media by which communication can be done through E-mails or SMS to stalk that person

A Cyber stalker is totally relies upon the consequence given by the internet, which follows them to stalk their victims without being detected. The cyber stalking is totally different from fake spam of various different messages by the spamming companies.

Let's find out what acts are considered stalking, how many types of stalkers are there, how Indian Law copes with stalking and some examples that will help in understanding stalking even better

Modes of stalking in India :-

1. Following a woman
2. Cyber stalking through different social media apps
3. Clicking photographs
4. Initiating a forceful conversation
5. Threaten of sexual assault
6. Sending unwanted messages
7. Spreading fake rumors

Cyber stalking includes :-

Cyber stalking is a crime where the attacker harasses the victim by stalking him/her over the internet. Cyber stalking includes browsing someone's online history with the help of social media and monitoring the activities of any person through the internet.

International Journal of Research in Social Sciences
Vol. 15 Issue 04, April 2025,
ISSN: 2249-2496 Impact Factor: 7.081 UGC Approved
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Types of stalkers :-

1. Rejected – The one rejected by the person he/she loved or was in a relationship with and experienced a breakup.
2. Incompetent suitor – The one who is incompetent at relationships and targets strangers or casual acquaintances.
3. Resentful – The one who feels they've been mistreated somehow.
4. Intimacy seeker – The one who is often mentally ill, the intimacy-seeking stalker believes the victim will love or learn to love them, and they may have a delusional belief that the victim already does love them
5. Political stalker – The one motivated by their political beliefs and ends up stalking people who agree or disagree with their views.
6. Hitmen – the one who stalks the victims by a hired killer who has instructions to badly injure or kill a person

Laws in India about cyber stalking :-

One example of this kind of cyber crime is cyber stalking, also known as online stalking or internet stalking. Cyber stalking, or the stalking of a person by electronic means (often the internet), is a kind of electronic harassment. Harassment takes many forms and might include monitoring someone's online behavior, making threats, stealing their identity or data, or even faking their data.

In cyber stalking, one individual illegally and repeatedly stalks another person via their online actions.

"Stalking is an obvious violation of Article 21 of the Indian Constitution, which protects the right to privacy. The case was Justice K.S,. Puttaswamy and Others vs. Union of India and Others and this was the decision." Its primary function is to make individuals feel afraid, but a secondary consequence is social isolation.

Negative mental states such as extreme narcissism, rage, vengeance, envy, obsession, and psychiatric condition, desire for control, sadomasochistic fantasies, sexual deviance, internet addiction, and religious fanaticism may all contribute to the development of stalker behavior. Different types of mental disturbance might lead to cyber stalking. A few examples are as follows:

1. Jealousy: Anxiety is an unpleasant feeling. Jealousy may play a role in a person's decision to stalk, particularly when it concerns a current or former romantic relationship.
2. Obsession and attraction: Stalking may also stem from unhealthy obsession or desire. The stalker could have an intensely emotional or sexual pull toward the target. There is a fine line between admiration and stalking.
3. Erotomania: As a kind of stalking, this theory holds that the target, who is often a stranger or a famous person, secretly has romantic feelings for the stalker. The attraction of a sexual nature is a necessary condition.
4. Sexual harassment: Sexual harassment is often believed to be the primary motivator for cyber stalking. The reason for this is that online life generally resembles the actual world.
5. Revenge and hate: The victim may not always be the initial inspiration for the stalker's feelings of rage and resentment, but he or she may nonetheless become the stalker' primary focus anyway. It would seem that the stalker uses the internet as a means of venting their rage and seeking revenge.

MUMAI KHANNA (not her real name), a worker at the American embassy in New Delhi, was unaware that her use of the internet might compromise her personal security. A man who appears to be cyber stalking 32-year-old Khanna asked her in a series of emails to strip for him or pay him Rs 1 lakh. "The woman said in her report to the Delhi Police that the threatening emails first appeared in the third week of November 2020.

Khanna was threatened by the defendant, who threatened to post her modified images and personal details (including her phone number and address) on sex websites. He allegedly threatened to distribute the photos widely in her southwest Delhi neighborhood.

"She initially ignored the emails, but she soon began receiving letters through posts, all of which had the same threat. She was compelled to report the incident to the authorities" stated an officer of the cybercrime cell. This was not the end of her ordeal, however. The accused lady received images of herself from the accused male through email. The lady said they were the same pictures she had kept in her mail. The authorities claim that the suspect gained access to the victim's personal images by cracking her email password. An initial inquiry following the allegation revealed that the victim's emails had originated from a cyber-café in South Delhi. Police Deputy Commissioner Dependra Pathak said, "We hope to locate the guilty as swiftly as possible" (crime). The suspect's apparent familiarity with the victim prompted law enforcement to conclude that the two knew one other.

Laws in India for Stalking and some of them with their Loopholes: -

A. Indian Penal Code, 1860

1. Section 354D of IPC

This of the Indian Penal Code, which criminalizes stalking, was added after the 2013 Delhi gang rape case. Both traditional stalking and newer forms of online harassment are discussed here. The scope of this section is articulated in terms of what constitutes "stalking." Anyone who tries to keep tabs on a woman's internet life is committing stalking, as the Section makes clear. Because of this, the stalker is breaking Section 354D of the Indian Penal Code if he commits any of the crimes described there.

- Loopholes

First, it ignores the possibility that males, too, might be victims by focusing only on "women" as victims. A violation of this clause constitutes cyber stalking if the offender tries to keep tabs on a woman' online activities using e-mail, instant messaging, or other electronic means. As we can see, it caters only to females. Therefore, the law is biased towards females. The second issue is that the lawmakers have not addressed the "means of monitoring." Although the individual may not want to stalk, his actions suggest otherwise.

2. Section 509 of IPC

Specifically, this clause may be used in the event of a man's violation of a woman's right to privacy, such as by sending her unwelcome electronic communications or making derogatory remarks about her online. Section 509 IPC may apply if he is found guilty of any of these acts.

- Loopholes

It is discriminatory towards men since it singles out women and ignores the fact that cyber stalking is a crime that affects both sexes equally.

In this paragraph, the words, voice, or gesture must be spoken out, heard, or seen. Cyber stalkers may easily circumvent the punishment imposed by this provision since they are unable to communicate with their victims in the usual ways (using words, gestures, and

sound) while communicating online. Finally, it is impossible to know whether or not a person communicating online has the goal of offending a woman's modesty.

B. Information Technology Act, 2000

1. Section 67 of the IT Act

Section 292A of the Indian Penal Code was used as the basis for this provision. Pornographic content in electronic format is discussed here. Therefore, the topic of cyber stalking will be discussed here. Stalkers may be prosecuted under Section 67 of the Information Technology Act if they use social media or other electronic means to broadcast obscene information about the victim with the intent to harass or intimidate that person.

2. Section 67A of the IT Act

In this Section, we discuss cyber stalking and its connected topics. The amendment of 2008 brought about the addition of this subsection. Section 67A of the Information Technology Act makes it illegal for a stalker to distribute "sexually explicit" information electronically (including through email, text message, or social networking site) and outlines the penalties for doing so.

3. Section 67B of the IT Act

The Amendment Act of 2008 initially included this particular Section. This section is dedicated to the topic of stalkers who prey on children under the age of 18 by spreading information showing minors engaged in sexual behavior for the express purpose of frightening them.

4. Section 66E of IT Act, 2000 and Section 354C of IPC

Voyeurism is addressed under both the Information Technology Act, 2000 (Section 66E) and the Indian Penal Code (Section 354C)."

A common tactic used by stalkers to make their victims feel uncomfortable and miserable is the release of intimate photos of them online. To make it illegal to publish or take images of a private act without the consent of the person is the purpose of both of these proposals. The victim in Section 66E is simply "any individual," but in Section 354C the gender of the victim is specified. In order to qualify as a "woman" under Section 354C, the victim must be one.

"What is remarkable here is that, while all offline regulations apply to digital media, the penalties under the IT Act are significantly more severe."

"It is worth noting that the IT Act places a strong emphasis on women's bodies and sexualities: Section 66A of the Act deals with a broad category of "offensive messages."

Section 354C of the Indian Penal Code outlaws voyeurism. Given that this provision applies only if the victim is a "woman," its scope is restricted. It is true that Section 354C of the Indian Penal Code prohibits voyeurism, but unlike Section 66E of the Information Technology Act, its reach is far narrower.

A victim under Section 66E might be anybody. Because of this, the victim's gender plays no role in determining whether or not this rule applies to them. Section 66E of the Information Technology Act of 2000 might be used by male victims to obtain compensation for their losses.

Present situation of cyber stalking :-

Cyber stalking, which may occur over the web or other technological means, falls within the scope of this provision as well. As the text of Section 507 of the law indicates, criminal intimidation by anonymous methods, it is clear that this section is meant to address the problem of stalking.

When the stalker has to hide his true identity in order to continue posing a danger to his victim, this tactic might be used. Penalties under Section 509 are intended for those who verbally or physically assault a woman's modesty. If he sends a lady repeated harassing communications through email or social media, he may be accountable for a privacy invasion on her part.

Although there is not a specific structure for this under the Information Technology Act of 2000. Publishing pornographic material online is addressed under Section 67 of the Information Technology Act, 2000. The wrongdoer will face legal consequences under this provision if he or she publishes defamatory material about the victim.

Transmission of sexually explicit material is addressed under Section 67A. It is possible to prosecute a stalker if he attempts to spread material that is overtly sexual in character. Section 66E of the IT Act, which mainly addresses voyeurism, may also be seen to include the act of stalking.

Kinds of Cyber stalking:-

Cyber stalking can be classified into three different types, which are as follows:

1. Email stalking;
2. Internet stalking;
3. Computer stalking.

Explanation ;-

- Email stalking

As with other forms of stalking such as phone calls, letters, and physical monitoring, email stalking has become more widespread in the real world. On the other hand, cyber stalking may take various forms. One of the most prevalent types of harassment is unsolicited electronic mail, which may include hateful, offensive, or even dangerous messages.

Other forms of electronic harassment include the sending of viruses or an excessive volume of junk mail to the victim. Note that spreading viruses or making telemarketing calls is not stalking in and of itself.

However, if such messages are delivered often with the intent to intimidate (much like physical-world stalkers who send victims pornographic magazine subscriptions), this might constitute stalking.

- Internet stalking

There is a real possibility that stalkers would use the internet extensively to spread rumors about their victims and put them in danger. In many cases, cyber stalking becomes more of a public issue than an individual one. This kind of online stalking is especially worrisome since it seems to have the most potential for expansion into real life.

Traditional stalking behaviors including persistent phone calls, graffiti, threatening letters, and even physical attacks sometimes accompany cyber stalking. The experiences of someone being stalked from 2,000 miles away and someone who is often within gunshot range of their stalker are quite different.

As a result of this, most criminal punishments take into account mental anguish, although it is not considered as harmful as a true physical threat. Internet stalking continues to concentrate on inflicting emotional distress, fear, and anxiety, despite experimental and real-world evidence linking stalking to domestic violence and feticide. This does not negate the need to punish those who intentionally cause fear and anxiety.

- Computer stalking

Finally, computer stalking is a subset of cyber stalking that involves gaining access to a victim's Windows PC via the victim's web browser. Few individuals are likely to be aware that any Windows PC with an active Internet connection may be found and linked to another computer remotely. With this connection, the hacker may take control of the victim's computer without any other parties getting in the way.

When a victim's computer establishes any kind of Internet connection, the cyber stalker is typically able to initiate direct communication with them. If a stalker has access to a victim's computer, the only way to protect oneself is for the victim to stop using the Internet and change their IP address.

Enforcement Problem

Section 75 "extraterritorial jurisdiction' is the primary obstacle to enforcing the Information Technology Act in India. This part makes it quite clear that anybody who commits a crime involving computer systems or networks in India, regardless of whether or not they are citizens of India, is liable to the provisions of the Information Technology Act. The scope of the legislation has to be expanded.

Furthermore, when the laws of two countries are in direct opposition to one another. In certain jurisdictions, stalking may be illegal but in others, the same behavior may not be considered criminal at all. As so, we have what is called a jurisdictional problem. As a result, there is an enforcement issue to consider. Both nations will benefit from working together to address this problem.

Recent steps taken in prevention of Cyber crimes:

The advent of computer era and Artificial Intelligence has revolutionized human life, shaping daily lives of everyone of us today. However, despite the numerous benefits, the misuse of computers and AI has given rise to cyber crimes, criminal activities committed through electronic means. While the IT Act, 2000 addresses various cyber crimes, this article focuses on the complementary role of the Bharatiya Nyaya Sanhita, 2023 (BNS) in providing punishments for specific cyber offenses

Initially, cyber crimes primarily occurred offline but evolved with technological advancements, posing threats to data privacy, social relations, and economic sovereignty. Examining the historical roots, the first cybercrime dates back to 1820 when Charles Babbage's invention of the computer witnessed sabotage by laborers. however, now cyber crimes are more often than not through online modes and with the thrust of the new criminal laws in India on digital investigations and trials, knowing about the penal liabilities on commission of cyber crimes becomes all the more necessary.

Laws relating to Cyber crimes under BNS:-

1. Section 294 of BNS:- Addresses the publication and transmission of obscene material, including electronically. The punishment includes imprisonment and fines, with harsher penalties for repeat offenses.

2. Section 77 of BNS:- Specifically deals with capturing or publishing pictures of private parts or acts of a woman without consent, constituting "voyeurism."

3. Section 303 of BNS:-This section specifically addresses theft related to mobile phones, data, or computer hardware/software. It offers a legal framework to prosecute individuals engaged in cyber theft activities. However, the applicability of special laws like the IT Act takes precedence in cases where they are attracted.

4. Section 78 of BNS:- Addresses the offence of stalking in both physical and cyber forms. Imposes imprisonment and fines for monitoring or bothering a woman through physical or electronic means.

5. Section 317 of BNS:- Applies when an individual receives stolen mobile phones, computers, or data. There is a punishment for even possession of such property, even by third parties.

6. Section 318 of BNS: Address frauds, including password theft, creation of bogus websites, and cyber frauds. Imposes varying imprisonment and fines based on the gravity of the offense.

7. Section 336 of BNS:- Deals with offenses like email spoofing and online forgery. Imposes imprisonment, fines, or both.This section also applies when forgery aims to harm a person's reputation.

8. Section 356 of BNS:- Penalizes defamation, including sending defamatory content through email. Imposes imprisonment and fines.

Punishment for cyber crime under IT Act:-

Data theft in India is primarily regulated by the IT Act, 2000. Within the IT Act, unlawful acts related to the disclosure of information in violation lawful contracts (Section 72A) and breaches of confidentiality and privacy (Section 72) are subject to penalties. Engaging in the unauthorized acquisition and use of a client's confidential customer or client list, resulting in a breach of confidentiality and privacy, may lead to liability under Section 72 of the IT Act, 2000.

Section 43 of the IT Act encompasses a range of activities falling under data theft. For instance, it specifies that individuals who, without proper authorization. download, copy, or extract data, computer databases, or information from a computer system or network, including data stored in removable storage media, are liable to compensate the affected party for damages.

Difference between cyber bullying and cyber stalking:-

Cyber bullying and cyber stalking are both harmful online behaviors that can have serious consequences for the victims. Cyber bullying involves the use of electronic communication to harass, intimidate, or threaten someone, often repeatedly and with the intention of causing harm. Cyber stalking, on the other hand, involves the use of electronic communication to

track, monitor, or harass someone in a way that instills fear or anxiety. While cyber bullying is more focused on emotional harm, cyber stalking can involve physical threats or actions. Both behaviors can have a significant impact on the mental health and well-being of the victims, and it is important for individuals to be aware of the signs and take steps to protect themselves online.

Comparison

• Attribute	Cyber bullying	Cyber stalking
• Definition	Harassment or bullying using electronic means	Repeated unwanted attention or harassment using electronic means
• Intent	Intent to harm, intimidate, or humiliate	Intent to control, monitor, or harass
• Frequency	Can be a one-time incident or ongoing	Usually involves repeated incidents
• Target	Targeted individual or group	Specific individual as the target
• Legal implications	May vary by jurisdiction	Illegal in many jurisdictions

Difference between cyber stalking and harassment:-
Cyber harassment and cyber stalking are both forms of online harassment, but they differ in their intent and severity. Cyber harassment typically involves repeated, unwanted communication or behavior that is meant to intimidate, annoy, or upset the victim. It can include sending threatening or offensive messages, spreading rumors, or posting embarrassing photos or videos. Cyber stalking, on the other hand, involves a pattern of behavior that is more malicious and intrusive, often including monitoring the victim's online activity, tracking their movements, or making threats of physical harm. Cyber stalking is generally considered more serious and can have a significant impact on the victim's mental and emotional well-being.

• Attribute	Cyber harassment	Cyber stalking
• Definition	Unwanted, repeated, and hostile behavior online	Intentional and repeated harassment or following of someone online
• Intent	May or may not involve a specific target	Specific target is usually identified and pursued
• Frequency	Can be occasional or frequent	Usually frequent and persistent
• Legal implications	May or may not be illegal depending on jurisdiction	Considered illegal in many jurisdictions

Summary with suggestions :-
Crime itself is a thrilling experience in everyone's life so to prevent crime we should take initiatives. Thus cyber crime is also a threatening to the society that we should be more

aware. Cyber stalking is a serious issue in India, and victims can seek legal recourse under various laws. It's essential to report incidents and take preventive measures to protect oneself from online harassment. Some of the aware steps are written bellow:

1. Individuals can guard against cyber stalking without losing their online independence. One strategy is to stay as anonymous as possible. Of course, complete anonymity is almost impossible on the internet nowadays, so the next best thing is to keep a low profile, especially on social media.

2. Rather than having an identifiable and traceable online presence, use nicknames and/or gender-neutral names when possible. Avoid posting personal details, such as your email address, home address, phone number or workplace details, online, where anyone can easily access them and use them to cyber stalk. Also, guard photographs, and make sure all private information, like vacation plans, photos and posts, are visible only to trusted individuals.

3. Use a primary email account only for communicating with known/trusted people and set up an anonymous email account for all other communications. Install email spam filters to minimize spam and the possibility of email-based phishing or cyber stalking attacks.

4. Update all software to prevent information leaks.
5. Mask your Internet Protocol address with a virtual private network, i.e., VPN.
6. Strengthen privacy settings on social media.
7. Strengthen all devices with strong passwords or, better, use multifactor authentication.
8. Avoid using public Wi-Fi networks.
9. Send private information via private messages, not by posting on public forums.
10. Safeguard mobile devices by using password protection and never leave devices unattended.
11. Disable geo-location settings on devices;
12. Install antivirus software on devices to detect malicious software.
13. Always log out of all accounts at the end of a session.
14. Beware of installing apps that ask to access your personal information.
15. Multifactor authentication types image Multifactor authentication requires using multiple factors to authenticate identity. These could include a password, a smart phone or biometrics, like fingerprints, face ID, etc.

We should thus stay aware to stay smart and safe. In the case of any mistake to do another we should step forward to law and thus also the appropriate authority.