

A LEGAL OUTLOOK ON WOMEN'S PREDICAMENT DUE TO CYBER STALKING

Sanjana Shikhar

ABSTRACT

With the multiple advancements of the internet, internet-related crime has spread its legs in all directions. Individuals are at tremendous risk from cyber-crime. Cyber stalking is the use of the web to track or threaten a person, group, or organization. Fake charges, surveillance, identity theft, threats, damage, and extortion are all options. Cyber stalking is frequently combined with real-time or offline stalking. A stalker could be a complete stranger on the internet or someone the target knows in person. They could be anonymous and ask people who aren't familiar with the target to participate. With the widespread use of computers and the progress of information technology, the risk of internet users has risen dramatically. Unfortunately, many people are unaware of the risks they are susceptible to while surfing the internet or saving data on their computers. Simultaneously, criminals exploit internet as a platform to engage in a variety of illicit operations against users. Traditional crimes like rape, molestation, and various forms of sexual abuse have taken on new meaning as a result of the advancement of information and communication technologies. There have been reports of rape scenes on mobile phone devices, as well as attempts to collect money by attempting to publish images/videos related to the incident. This paper aims to provide readers with a thorough understanding of cyber stalking and women's plight as a result of it by going over the concept of cyber stalking, causes, identification, consequences, legal remedies available and some suggestions for the same.

Keywords: Cyber Stalking, Law, Harassment, Stalker, Online, Internet, Cyber Space



INTRODUCTION

A 21-year-old lady saw an image of her face digitally placed on the body of another woman posted on a social media platform in the Salem region of Tamil Nadu in June 2016. She told her parents, as well as identified the perpetrator. He allegedly modified her photograph using a mobile phone app, posted it to the site, and tagged her in the post after she refused his marriage proposal. A complaint was filed with the Cyber Crime Cell by the woman's father. She discovered another distorted photograph linked to her social networking account a few days later, this time with her name and her dad's phone number. The woman committed suicide on the same day. She stated her utter ignorance of the skewed visuals in her suicide letter, as well as her inability to persuade anyone.¹

The Information Technology Act of 2000² established a number of cybercrime offences. Among the many objectionable activities on the internet, online abuse is a worldwide issue that has directly or indirectly harmed online users of all ages, resulting in various forms of harassment such as gender bullying, stalking, trolling etc. A person's repetitive, unsolicited, hostile activity through cyberspace with the goal to fear, intimidate, humiliate, threaten, harass, or stalk someone else is known as cyber harassment.³ Apart from physical harassment being a crime under Indian law, harassment perpetrated through electronic media such as social networking sites, chat rooms, and e-mail is also deemed to have the same legal consequences as traditional harassment offences. Women in India, according to popular belief, are the most vulnerable targets on the internet and in digital communication technologies because of their gender and the popularity of pornographic photographs of Indian women.⁴ Women are frequently the subject of such unusual behaviours in order to smear the image of their immediate family members. However, a number of cases go unreported, either because of a lack of awareness or because there are no strict rules in place to deal with them. It's also worth noting that just a few of cases of this sort are really documented and prosecuted. Furthermore, since the Supreme Court's ruling in Shreya Singhal v. Union of India, ⁵ which struck down Section 66A⁶ of the

¹A Girl Hanged Herself In Tamil Nadu Over Morphed Obscene Photos of Her on Facebook, available at: https://www.scoopwhoop.com/A-Girl-Hanged-Herself-In-Tamil-Nadu-After-Morphed-Obscene-Photos-Of-Her-Were-Posted-On-Facebook/ (last visited on Jan. 16, 2022).

² The Information Technology Act, 2000 (Act 21 of 2000).

³Internet Harassment- Cyber stalking, Cyber harassment and Cyber bullying, available at: https://astrealegal.com/internet-harassment-cyber-stalking-cyber-harassment-and-cyber/ (last visited on Jan. 16, 2022).

⁴ DEBARATI HALDER & H. JAISHANKAR, Cyber Crimes Against Women in India (Sage Publications Pvt. Ltd, India, 2016).

⁵ (2013) 12 SCC 73.

⁶ The Information Technology Act, 2000 (Act 21 of 2000), s. 66(A).



Information Technology Act, 2000, there has been a gap in the legislation to address such offences. The verdict, which focused on the fundamental right to freedom of speech and expression, stated that liberty of thought and expression is more than a lofty ideal.

MEANING, IDENTIFICATION, REASONS AND THE POSSIBLE CONSEQUENCES OF CYBER STALKING

MEANING OF CYBER STALKING

A research paper titled "Stalking Strangers and Lovers" published in 1995 was one of the first to use the term "stalking" to describe the regular phenomenon of males aggressively pursuing their female former partner following a breakup. Prior to that publication, the terms "female harassment", "obsessive following" and "psychological rape" were more typically used instead of "stalking."⁷

The term "stalker" was first used by the press in the twentieth century to characterize those who worry and harass others, initially with reference to strangers who were portrayed as "obsessed" with celebrities. It has been in use since at least the 16th century to relate to a prowler or a poacher. The tabloid press in the United States appears to have created this usage of the term. With time, the definition of stalking evolved to include people who were hounded by their former relationships. Pathé and Mullen describe stalking as a constellation of actions in which an individual perpetrates upon another numerous unwanted intrusions and communications. The purposeful and repeated following, watching, or pestering of another person is known as stalking. Stalking differs from other crimes in that it is a sequence of activities that take place over a long period.8

Cyber stalking refers to the use of cyber platforms, such as social media and various network modes, to conduct illegal surveillance. Stalking is a serious criminal offence since the phrase itself implies that it is an illegal act. As a result, cyber stalking ipso facto becomes a crime with serious penalties.

The term "cyber stalking" refers to computer-assisted harassment. A cyber stalker does not make a direct physical threat to the victim, but instead threatens them online or intimidates them verbally. In cyberspace, it is a continual function. The word "cyber stalking" encompasses a large number of

⁷Stalking, available at: https://en.wikipedia.org/wiki/Stalking (last visited on Jan. 16, 2022).

⁸ Ibid.

⁹Cyber Stalking: Challenges Regulating Cyber Stalking at the Cyber in Space, https://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyberspace.html (last visited on Jan. 16, 2022).



different types of criminal activity. The use of electronic methods to stalk or harass an individual, a group of individuals, or a certain class of people is known as cyber stalking. After a thorough investigation, it was discovered that cyber stalking is frequently carried out with the intent of falsely accusing, coercing, threatening, or vandalizing a person. It's frequently used for identity theft, coercive manipulation, and blackmail.

In the year 2001, the Delhi cops arrested Manish Kathuria for impersonating a lady in an Internet chat room, which was the first incidence of cybercrime and cyber stalking to be reported and punished. Kathuria was charged with outraging the modesty of his victim Ritu Kohli under Section 509¹⁰ of the Indian Penal Code. ¹¹However, the Indian Penal Code in 2001 did not include all of the remedies for cyber-crime, stalking, and harassment.

Ms. Kohli was obliged to migrate out of India due to the insufficiency and lacunae of legal remedies, according to Pavan Duggal, a Delhi-based Cyber Law specialist who works on this issue. After Nirbhaya's case¹², the Indian Penal Code was modified in 2013 to add stalking as a criminal offence.¹³

METHODS AND REASONS BEHIND CYBER STALKING

WAYS TO COMMIT CYBER STALKING

- a. By observing the victim's actions and monitoring her online activity, the stalker acquires all of the victim's details.
- b. The stalker has amassed a dossier on the victim and threatens to utilise it for his own personal gain.
- c. He then publishes it on the web and asks people to have sexual relations with the victim.
- d. People of all kinds start calling the girl and forcing her to do things she doesn't want to do, including sexually harassing her.
- e. Enter the victim's e-mail address into pornographic and sex sites.¹⁴

¹⁰ The Indian Penal Code, 1860 (Act 45 of 1860), s. 509.

¹¹ The Indian Penal Code, 1860 (Act 45 of 1860).

¹² (2017) 6 SCC 1.

¹³What is Cyber Stalking and its Legal Remedies in India?, available at: https://www.how2shout.com/news/cyberstalking-and-its-legal-remedies-in-india.html (last visited on Jan. 16, 2022).

¹⁴Supra note 9.



REASONS BEHIND CYBER STALKING:

HARASSMENT:

The stalker's main goal is to harass the target. In one case in the United States, the stalker was victim's neighbor, and he possessed her semi-naked photo and taking advantage of which the stalker threatened the victim to have sex with him or he would post the photo on social media. He harassed her for a year in this manner, after which her parents discovered it and reported it to the police. That photo was taken from the victim's social media account and morphed into a semi-naked photo of the victim.¹⁵

MONETARY GAINS:

Cybercrime, like many other types of crimes, is primarily motivated by monetary gain. Cyber thieves typically demand money by pressuring or coercing the victim to post private photos or videos taken by them using multiple internet identities.¹⁶

FASCINATION:

This is referred to as one-sided love or internet romance. The person would be having feelings for the victim and will become her stalker if she refuses to accept his proposal. He would be unable to accept the ending of his relationship. The victim may even be murdered by the accused in this situation. In 2012, a college girl in Tamil Nadu was attacked with acid by her one-sided lover. This is not really stalking, but it's been observed that some of these people also become stalkers.¹⁷

REVENGE

Even though the victim is not the source of the stalker's feelings of hatred and revenge, yet she remains the stalker's target. The stalker seems to consider the web to be the handy outlet for venting his rage. The victim in a case from Germany refused to accept the stalker's request. As a kind of retaliation, he posted her photo on social media with the phrase 'if anyone wants to have sex, call me,' along with her address and phone number. The victim was completely unaware of the situation. As a result of

¹⁵ CYBER STALKING, available at: https://aishwaryasandeep.com/2021/06/21/cyber-stalking/ (last visited on Jan. 16, 2022).

¹⁶ The Motives Behind Cyber Crime, available at: https://gramener.com/blog/posts?post=08-21-2015-cyber-crime-themotives.md (last visited on Jan. 16, 2022).

¹⁷Supra note 15.



that post, a large number of people contacted her, and some even came to her house in the middle of the night and sexually harassed her.¹⁸

BOASTING OR SHOWOFF

This is a form of show-off to demonstrate that the stalker has the ability to harass a girl. This occurred among a group of friends. The stalker challenged his friends, claiming that he could make the girl cry in no time. However, these kinds of tasks might be perilous at times.¹⁹

IDENTIFICATION AND DETECTION

In cyber stalking, a number of significant elements have been found. 20 They are as follows:

- 1. Fake allegations: Many cyber stalkers attempt to smear their victim's reputation and turn others against them. On the internet, they spread fake information about them. They can do this by creating their own websites, blogs, or user pages. They make claims about the victim on newsgroups, chat rooms, and other public-access websites.
- Attempts to gain personal information from the victim: Cyber stalkers may contact their victim's friends, relatives, or coworkers in order to obtain personal information. They could use the Internet to advertise for information or hire a private investigator.
- 3. Observing their targets' internet activities and trying to track down their IP address in order to learn more about them.
- 4. Encourage others to target the victim: Most cyber stalkers attempt to enlist the help of others to torment the victim.
- 5. The cyber stalker would blame the target of disturbing him or her without evidence.
- 6. Attacks on data and equipment: They may attempt to corrupt the victim's computer with viruses.
- 7. They place orders in the victim's name for products and services, such as magazine subscriptions. Common instances include membership in pornography or ordering stuff and having them delivered to the victim's office.
- Scheduling a meeting: Young people are particularly vulnerable to online stalkers attempting to arrange encounters between them.

¹⁸ Ibid.

²⁰Cyber Stalking, available at: https://en.wikipedia.org/wiki/Cyberstalking#Definitions_and_description (last visited on Jan. 16, 2022).



9. Making defamatory or insulting statements on the internet or on message boards in order to elicit a response or reply from their target.

IMPACT OF CYBER STALKING ON WOMEN

Women and small children are frequently the victims of such activities, which result in threats, harassment, violence, and trauma. Women are the most impacted community in this regard, as privacy in the virtual world as well as in real life is increasingly dwindling. Cyber stalking is a significant example of women's online privacy being violated. ²¹ Furthermore, given the nature of the act and the intended target, such anomalous behaviors have a profound impact on every part of their lives. According to Pulkit Sharma, a clinical psychologist in Delhi, when someone tries to bully you online, it is seen by a much bigger audience and you feel powerless since you can't stop the spread of incorrect information or a photograph. As a result, the sensation of guilt, trauma, and being exposed is much, much higher. ²² Majority of these crimes go undetected, either by police or by the victims' relatives, because they believe the harassment is regretful but not truly punishable. Even while there are rules prohibiting internet harassment, it is the enforcement of these regulations that is the issue. Some of the physical and mental consequences of cyber stalking²³ are as follows:

A. Denial, bewilderment, and self-doubt, as well as a questioning of whether or not what is occurring is reasonable, and whether or not they are overreacting.

- B. Difficulty concentrating, paying attention, and recalling information.
- C. Sleeplessness nightmares, rumination
- D. Irritability, rage, and homicidal ideas.
- E. Insecurity and a lack of trust in others, as well as intimacy issues.
- F. As a result of growing more distrustful, introverted, or aggressive, one's personality changes.

²¹Dr. S.K. Mohapatra, "Victimization of Women Under Cyberspace in Indian Environment" 2 International Journal of Academic Research 221 (2015).

²² Cyber Stalking in India, available at: https://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html (last visited on Jan. 16, 2022).

²³ Impact of Stalking on Women, available at: https://www.stalkingriskprofile.com/victim-support/impact-of-stalking-on-victims (last visited on Jan. 16, 2022).



- G. Lack of sleep causes fatigue, a constant state of vigilance, and emotional distress.
- H. Headaches and hypertension are some of the side effects of prolonged stress.
- I. Insecurity and a lack of trust in others, which has an impact on existing and future friendships and relationships.
- J. Others detaching from the victim since they don't believe the victim, or because they can't cope with the victim's mental state, or as a direct result of third-party victimization.

Besides this, trolls, bullies, and stalkers harass women on the internet with insulting, libellous, and disparaging statements/pictorial depictions. Women may be harassed and hounded by unwanted phone calls and SMSs even if they are not connected to the internet. This can occasionally lead to women being fully barred from utilizing any form of communication, which is a clear violation of women's rights due to the incorrect exercise of their freedom to speech and expression on the internet. They are a violation of core human rights, such as the right to equality given by Article 14²⁴ of the Indian Constitution²⁵ and the right to live in dignity guaranteed by Article 21²⁶ of the Constitution. Unfortunately, when deciding the constitutionality of Section 66A of the IT Act, 2000 in the court decision of Shreya Singhal v. Union of India,²⁷ the Supreme Court emphasized the right to freedom of speech and expression, but ignored the stigmatization of women in cyberspace as a result of the abuse of this right.

LEGAL REMEDIES AVAILABLE

Section 354²⁸ of the Indian Penal Code, 1860, is one of the most essential judicial remedies. Following the horrible Nirbhaya tragedy, the Criminal Law (Amendment) Act, 2013, was passed, which includes various measures under the Indian Penal Code aimed at improving women's safety, security, and protection.

A. Stalking is punishable under Section 354D²⁹ by jail term of either description for a period that may stretch to three years, and also a fine, on a first guilty verdict; and on a second or

²⁴ The Constitution of India, art. 14.

²⁵ The Constitution of India

²⁶ The Constitution of India, art. 24.

²⁷ Supra note 5.

²⁸ The Indian Penal Code, 1860 (Act 45 of 1860), s. 354.

²⁹ The Indian Penal Code, 1860 (Act 45 of 1860), s. 354D.



subsequent conviction, by jail term for a term that may extend to five years, as well as a fine. Even though the person stalked has disallowed it, such a stalking operation had to be carried out. Furthermore, if the stalker can show that the activity was carried out only to warn the former of the possibility of a crime being committed against him/her and in good faith, the stalker's culpability under Section 354D can be voided.

- **B.** Section 292³⁰ of the Indian Penal Code, 1860, governs the publication of immoral material with the intent of blackmailing the intended victim.
- **C.** The IPC Section 499³¹ deals with defamatory messages sent via email or any other social networking platform.
- **D.** Sections 507³² and 509³³ of the Indian Penal Code, deals with illegal pressure by anonymous communication and maligning women's modesty.

There is no legal provision for internet stalking in the Information Technology Act of 2000. This is because when a someone is stalked via network/social media, there must be proof of the stalking, which usually comes in the form of annoyance, defamation, forgery, information leaking, and other forms of harassment. The Information Technology Act of 2000 makes certain practices illegal.

- **A.** According to Section 67³⁴ of the Information Technology Act of 2000, anyone who transmits or causes another to transmit any obscene or material of sexual connotation is punishable on a first guilty verdict by jail term for a term up to three years and a fine up to five lakh rupees, and on a second or subsequent conviction by imprisonment of either description for a period up to five years and a fine up to five lakh rupees.
- **B.** Under section 67A³⁵ of the Information Technology Act of 2000, anyone who publishes, transmits, or causes to be published or transmitted in electronic form any material containing explicit sexual act or behavior is punishable on a first guilty verdict by imprisonment of either description for a term up to five years and a fine up to ten lakh rupees, and on a second or subsequent conviction by imprisonment of either description for a term up to five years and a fine up to ten lakh rupees.

³⁴ The Information Technology Act, 2000 (Act 21 of 2000), s. 67.

³⁰ The Indian Penal Code, 1860 (Act 45 of 1860), s. 292.

³¹ The Indian Penal Code, 1860 (Act 45 of 1860), s. 499.

³² The Indian Penal Code, 1860 (Act 45 of 1860), s. 507.

³³ *Supra* note 10.

³⁵ The Information Technology Act, 2000 (Act 21 of 2000), s. 67(A).



- **C.** Under section 72³⁶ of the Information Technology Act of 2000, anyone who obtains access to any electronic record, book, register, correspondence, information, document, or other material without the permission of the person and discloses such electronic record, book, register, correspondence, information, document, or other material to any other person, faces up to two years of prison sentence and penalty of up to one lakh rupees.
- **D.** With the revision of the IT Act in 2008, Section 66A³⁷ was added to the IT Act, which dealt with all incidents of cyber stalking.

As per Section 66A of the IT Act, anybody who communicates, using a computer resource or a communications system, any information that is grossly offensive or menacing in nature or any information that he knows to be false, but persistently sends through such computer resource or communication device for the purpose of causing irritation, inconvenience, threat, interruption, insult, injury, criminal intimidation, enmity, hostility, or ill will or any e - mail or electronic mail message sent with the intent to harass or inconvenience the addressee or receiver, or to deceive or mislead them about the source of such messages, shall be punished by imprisonment for a period of up to three years, as well as a fine.

In a significant development and amid controversy, Section 66A was recently struck down by the Indian Supreme Court in Shreya Singhal case³⁸ (decided on March 24, 2015), having declared it to be in direct contravention right to freedom of speech and expression stated in Article 19(1)(a)³⁹ of the Indian Constitution.

The Supreme Court ruled in the case that the increased availability of information via the internet cannot be used to limit the substance of the right in Article 19(1)(a), nor can it be used to justify its rejection. However, we disagree with attorneys for the Petitioners that there is no discernible difference between print, broadcast, and real-time speech and speech on the internet when it comes to discrimination under Article 14. The discernible difference is clear: the internet provides anyone with a platform to broadcast his or her opinions for very little or no cost. As the erudite Additional Solicitor General correctly noted, something uploaded on a webpage or website spreads like lightning

³⁶ The Information Technology Act, 2000 (Act 21 of 2000), s. 72.

³⁷ Supra note 6.

³⁸ Supra note 5.

³⁹ The Constitution of India, art. 19(1)(a).



and can reach millions of individuals all over the world. If the Petitioners are accurate, this Article 14 point would be applicable to all other charges imposed by the IT Act that aren't questioned in these petitions. We demonstrate that there is a discernible difference between speech on the internet and speech on other forms of communication, and that discrete offences can be created by legislation. As a result, we conclude that the challenge based on Article 14 must be dismissed.⁴⁰

RELEVANT CASES WITH REGARD TO CYBER SECURITY

CASE OF MANISH KATHURIA

As previously stated, in India, the first instance of cyberstalking was reported in the year 2001. Manish Kathuria was stalking an Indian woman named Ms. Ritu Kohli by illegally conversing under her name on the website www.mirc.com and using filthy and offensive language, as well as circulating her home phone number and asking people to call her. As a result, for three days in a row, she received over forty lewd phone calls at odd hours of the night. She was obligated to approach the Delhi Police Department as a result of the circumstance. As soon as the complaint was submitted, Delhi Police identified IP addresses and arrested Kathuria under Section 509 of the Indian Penal Code. The IT Act was not used in this instance since it had not yet come into existence when the complaint was filed. While no further action has been taken, this issue has caused Indian legislators to notice the need for cyber-stalking legislation. ⁴¹

KARAN GIROTRA V. STATE

Shivani Saxena was the women involved in this case, who sought a divorce by unanimous understanding after her wedding could not be consummated. She met Karan Girotra over the internet during this period, and he told her he loved her and wanted to get married to her. Under the pretence of showing Saxena to his family, Girotra drugged her and sexually assaulted her at his home. He started sending her filthy images from the point of time she was attacked and continuously persuaded her to marry him. Unless she married him, he allegedly threatened to make the photographs public. As a result, the two conducted an engagement ceremony, but he repeatedly used to beat her and ultimately ended their engagement. As a result, Saxena filed a complaint under Section 66-A of the IT Act.

-

⁴⁰Shreya Singhal v. UOI ON 24 March, 2015, available at: https://indiankanoon.org/doc/110813550/ (last visited on Jan. 16, 2022).

⁴¹Supra note 9.



Regardless of the fact that the Court denied Girotra's request for anticipatory bail on the basis that Girotra shared naked and obscene photos of Saxena, an offence that merits harsh custody interrogation, it made some disparaging remarks. According to the Court, Saxena did not reveal her prior marriage to Girotra just because she agreed to execute the engagement ceremony, despite the fact that Girotra had mentioned it when he initially expressed his love for Saxena. The Court also noticed Saxena's tardiness in filing the FIR. What's more astonishing is that the Court determined that Saxena had agreed to the sexual activity and only filed the complaint after Girotra denied to marry her.⁴²

CASE OF YOGESH PRABHU

Despite the fact that the conviction rate for cyber stalking has been low since the modifications to the IT Act took effect in 2008, the Mumbai cyber cell obtained the first ever conviction under the IT Act in Maharashtra in July 2015. In 2009, the cell looked into the matter of online stalking. Yogesh Prabhu was found guilty of stalking and sending obscene photographs to his coworker by a metropolitan magistrate court. Under sections 66-E (penalty for infringement of privacy) of the Information Technology Act, 2008 and section 509 (word, gesture, or act designed to offend the modesty of a lady) of the IPC, the court sentenced him to three years in prison and a fine of Rs. 10,000 and Rs. 5,000, respectively. The conviction was based on evidence that included a key witness statement claiming that the offence was performed using an office-sponsored laptop. 43

VINU PRIYA CASE

As previously stated, the victim in this case was a 21-year-old woman who had recently completed her education. She informed her parents on June 23, when the first photos appeared, and they filed a complaint with the Cyber Crime Cell. The police promised Vinu Priya's father that the offender would be apprehended in two weeks, either because they lacked the investigative abilities to track down the source of the modified photos or because they were simply uninterested. If the parent wanted the inquiry to be completed, one of the officials in the Cyber Crime Cell reportedly asked for a mobile phone. Vinupriya's father claims he purchased the constable a mobile phone valued Rs 2,000 and that the officer did not provide justice after taking a bribe. On June 26, Vinu Priya was terrified after

⁴²Ibid.

⁴³Cyber cell's first conviction: Man gets 3 years for sending obscene messages, stalking colleague, available at: https://indianexpress.com/article/cities/mumbai/cyber-cells-first-conviction-man-gets-3-years-for-sending-obscene-messages-stalking-colleague/ (last visited on Jan. 16, 2022).



another disgusting photograph was posted on Facebook. Previously, the investigating officer suspected she had sent those images to someone, but they were now being disseminated, presumably by a betrayed lover. These were Vinu Priya's lines of questioning. She killed herself by suicide while she was alone at her residence on June 27. The second photograph, which first circulated on June 26th, was removed within hours of Vinu Priya's death being confirmed. This proved that the predator was either hiding nearby or among Vinu Priya's acquaintances.⁴⁴

CHALLENGES IN PREVENTING CYBER STALKING

Following are some of the challenges involving cyber stalking:⁴⁵

- **A.** Wrongdoer's Anonymity: One of the most important aspects of the internet is its capacity to keep users anonymous, which is thought to be useful to perpetrators because it allows them to keep their identities hidden.
- **B.** Investigation capabilities are in a bad state: India's cyber-crime investigation capabilities are likewise in a bad shape. There is no appropriate infrastructure in place to deal with technological crimes. As a result, the prosecution's case is weaker due to a lack of acceptable evidence.
- C. Increasing Risks on Online Means: Because the internet has no limits, it has a larger audience, and harassment, abuse, and other issues can be seen by individuals in different parts of the world. Furthermore, sophisticated technology has the potential to morph images, change voice, and other aspects of the internet, potentially causing major societal disorder. The internet opens even more opportunities to intrude people's privacy and infringe Article 21's core rights to life, liberty, and dignity.
- **D.** Society's Barriers: In addition to technological hurdles, women face various forms of prejudice as a result of the society's dominant patriarchal nature. The term 'ladylike modesty' is a relative term that differs from one community to the next. There have been various

_

⁴⁴Supra note 9.

⁴⁵Archana Sarma, "Cyber Stalking and the Plight of Women in India- A Legal Perspective" 9 Ram Manohar Lohiya National Law University Journal 190 (2017).



incidents where society has held victims responsible for uploading images on social networking platforms that are deemed 'questionable' by the society. This exacerbates the issue.

CONCLUSION AND SUGGESTIONS

The number of internet-related crimes has increased dramatically, as have the intricacies of criminal behavior, thanks to the evolution of online communication. The capability of the human mind is unfathomable. Cybercrime will never be totally eradicated from the internet. It's possible to investigate them. No law has ever managed to totally eliminate crime from the world, as we can see gather from our past experiences. The only way to prevent crime is for individuals to be educated regarding their rights and obligations, and for laws to be enforced more harshly. The internet and internet-related crimes are on the rise at an alarming rate. The sections on cybercrimes are not exhaustive. By way of amendments, a slew of new provisions is inculcated on a regular basis. Dealing with cyber-crime was particularly difficult prior to the passage of the IT Act in 2000. Since its inception, it has been actively used to provide victims of cyber-crime with potential remedies, giving a larger segment of the population hope that, in recent years, the growth of network systems will be supplemented by the development of stringent laws, reducing the likelihood of any cyber-crime occurring.

However apart from legislations, some suggestions which should always be followed are given here below:

- A. When stalking occurs in cyberspace, the server of the electronic equipment used to carry out the stalking may be located outside of India's territorial jurisdiction. As a result, if service providers are required to establish a local server in India, it may be possible to investigate such incidents. Such an approach might be able to handle the issue of jurisdiction in such circumstances to some extent.
- B. There is a need to develop high-level security measures that are comparable to those used around the world.
- C. A few preventive steps include updating antivirus software on a regular basis, resetting passwords, and updating the operating system.
- D. There is a huge need for public awareness, IT education, and training.



- E. If you want to establish a professional online presence, it's best to keep all of your posts on the Professional account focused on the task you want to promote rather than your personal life. However, the personal account you made primarily for communicating with friends, coworkers, or relatives should remain in private mode, and you should be cautious when accepting requests from strangers.⁴⁶
- F. Many social media networks allow users to publish their live whereabouts or tag the real location they are in, which might put them in dangerous circumstances.
- G. Someone you met on media platforms or through an online dating app should not be met in person.
- H. Keep the GPS location on your phone or other equipment turned off when you don't need it.
- I. Responding to unknown people's messages can often provoke a stalker, whose hidden purpose is to draw your attention. Alternatively, you can gently request that they stop sending such texts and inform them of the legal ramifications if they do not comply.⁴⁷
- J. As soon as possible, suspicious people should be blocked from one's social network account.
- K. Keep an eye out for phone/email messages that aren't relevant or are fake.
- L. Do not reply to emails that request personal information.
- M. Be wary of phishing websites that attempt to steal private information.
- N. Keep an eye out for privacy policies on websites and apps.
- O. Keep your email address safe.
- P. Make your passwords as strong as possible.

Cyber stalking has emerged as a new menace to India's cyber community, particularly women, regardless of their age or socioeconomic status. It has even resulted in the deaths of a number of young ladies. As a result, it is imperative that India develop a technically proficient legal framework as well as an unbiased procedure for properly resolving incidents of cyber stalking.

_

⁴⁶How to prevent Cyber Stalking, available at: https://blog.ipleaders.in/how-to-prevent-cyberstalking/#Keep_your_professional_account_different_from_your_personal_account (last visited on Jan. 17, 2022). ⁴⁷Ibid.