INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 2

2020

Cyber Stalking Issues of Enforcement in Cyber Space

VIOLA RODRIGUES[1]

ABSTRACT

As new technologies and innovations emerge, there has also been a shocking rise in crime around the world and cybercrime is now one of the most vulnerable crimes. The cyberspace is taken up by a new form of crime which involves repeated attempts by one person to reach another, causing that person a sensation of threat in his or her mind. This emerging crime is commonly referred to as cyber stalking. India too is no exception in this paradigm of cyber crime. This crime have created new issues and challenges for the detection, and prevention of such crimes as it is inadequate to just use the traditional methods such as identification by witnesses and enforcing restraining orders. In this crime of cyber stalking, cyber stalker disguise themselves using the internet without the fear of any consequence and target victims. This paper examines cyber stalking as an example of a crime that is simultaneously both amenable to, and resistant of, traditional forms of legislation, depending upon the way in which the possibilities of the Internet are exploited. The paper attempts to define cyber stalking first and then explains different manners of stalking. There is a distinction made between cyber stalking and offline stalking. The more focus has been laid down on Indian legislative framework regarding cyber stalking and drawbacks concerned to it. The constitutional framework with respect to cyber stalking has also been discussed. In the latter part, the paper attempts to suggest measures to prevent the crime and deal with cyber stalkers.

Keywords: *Cyber crimes, Cyber stalking, Cyber space, challenges, framework, Internet.*

I. INTRODUCTION

Our life has improved in countless ways through the advent of new technologies and inventions. Technology developments not only extend the scientific frontier, but also question the legal framework. The information technology is collectively called computers, the internet and cyber space. The digital world primarily uses Internet and cell telephones in information technology. IT has evolved and has become the foundation for economic and technical growth today. The internet universe provides every user with all the required details. With the various developments in the Internet, cyber crime has also broadened its reach and it poses a huge

[1] Student of School of Law, CHRIST (Deemed to be University), India.

 [ISSN 2581-5369]

threat to the community. Among various cyber crimes, one such is cyber stalking. It is the use of the internet or other electronic means to stalk or harass a person. *Cyber Stalking involves following a person's movements across the internet by posting messages in the nature of threatening on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc*[2].

Cyberstalking is a new genus of crimes that existed since the late 1990's that emerged as major international criminological issues[3]. In essence Cyberstalking describes the use of information and communication technology in order to harass one or more victims[4]. Harassment also includes any behaviour, whether deliberate or not, that causes the victim's distress. Cyberstalking uses computers and networks for illegal behaviour, frequently locating its target online, as these tools can easily be used to threaten, bully, coerce, harass and assault unsuspecting users[5].

Cyberstalking is similar to conventional stalking methods as it involves repetitive actions causing fear and apprehension. Nevertheless, as new technology arise, conventional stalking has taken on entirely new forms through different means, such as e-mail and the Web, i.e. cyberspace. Cyberstalking significantly shows the internet's capacity for encouraging such forms of crimes and points to accessible and potentially successful solutions. Cyberstalking is a radically new type of deviant behaviour that uses technology to threaten others. In a decade, Cyberstalking has become a rising social issue with computer users all over the world due to our dependency on Internet, e-mail, instant messaging, chat rooms and other communication technologies. Online-interaction anonymity decreases the risk of recognizing and increases the use of cyber stalking. Although cyber-stalking can seem fairly harmless, it can cause psychological and emotional damage to the victims. Occasionally this can escalate to real stalking. Cyber stalking is becoming a common tactic in racism and other expressions of intolerance and hatred in today's information society.

Tackling information technology is the present challenges for law. These problems are not limited to any particular conventional category of law but to almost every category of law. When dealing with information technology, the current legal system and frame work have proven inadequacy. It requires new definitions and understanding of accepted standards of criminal conduct and punishment. In the context of cyber-space criminal activity, legal laws

[2] Abhijeet Deb, *Cyber Crime and Judicial Response in India*, 3 Indian J.L. & Just. 106 (2012).
[3] JAISHANKAR, K., INTERNATIONAL PERSPECTIVES ON CRIME AND JUSTICE 541-556 (2004).
[4] BOCJJ P., THE DARK SIDE OF THE INTERNET: PROTECTING YOURSELF AND YOUR FAMILY FROM ONLINE CRIMINALS 159-161 (2nd ed., Green Wood Publishing Group, Westport, CT) (2006).
[5] MORLEY, D., UNDERSTANDING COMPUTERS IN A CHANGING SOCIETY 196-199 (3rd ed., Course Technology Cengage Learning, Boston, MA) (2008).

 [ISSN 2581-5369]

can be governed, administrative framework function can be improved, and the accused can be prosecuted in accordance with the fast and effective delivery mechanism. Such issues have been discussed by the judiciary worldwide.

Thus this paper will explain the concept of Cyber stalking and the different manner of stalking adopted by the stalker to harass the victim. In the following chapter, distinction will be made between cyber stalking and offline stalking. The paper then explains about the role of Indian legislative framework in curbing these types of cybercrimes which has a serious impact on society affecting people both physically and mentally and analyses the drawbacks concerned to it. The paper also explains Indian constitutional framework with respect to cyber stalking.

II. DEFINING CYBER STALKING:

"Cyber Stalking" is defined as a crime where the stalkers use internet or any other electronic device to stalk someone[6]. Online harassment and online abuse are synonymously used for cyber stalking. It involves the conduct of repeated harassment or threats to an individual. Stalking can be done in the following ways such as: to follow a person to his or her home or business, destroy the property of a person, leave written messages or objects, or making harassing phone calls. The cyber stalkers always believe they are anonymous and they can hide. In other words, the biggest strength of the cyber stalker is that they can rely on the anonymity that internet gives them to keep a check of their victim's activities without detecting their identity. Therefore, efficient cyber tools are needed to investigate cyber-crimes and to be prepared to defend against them and bring victims to justice.

The definition of cyber stalking has academically been interpreted primarily by digital communication technology as sexual harassment. Bocij, Griffiths and McFarlane define cyber stalking as *"a group of behaviours in which an individual, group of individuals or organization, uses information and communications technology to harass one or more individuals. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes and confrontation"*[7].According to Baer, *"Cyber stalking in particular is composed of words alone and therefore stands more distinctly as apart as a crime of accumulation"*[8]. Ellison and Akdeniz, had construed the term cyber stalking as *online harassment, which may include various digitally harassing*

[6] Heena Keswani, *Cyber Stalking: A Critical Study*, Bharati Law Review.131, 131-32 (2017).
[7] Bocij, P., Griffiths, M.D., McFarlane, L, *Cyber Stalking: A New Challenge for Criminal Law*, 122 The Criminal Lawyer, 3-5 (2002).
[8] Baer, M., *Cyberstalking and the Internet Landscape we have constructed*, 15 Va. J.L. & Tech, 154-172 (2010).

 [ISSN 2581-5369]

behaviours, including sending junk mails, computer viruses, impersonating the victim, etc[9].

It may be noted that, legally, cyber stalking was recognised as an offence only in the early 1990s. Stalking through cyber space was criminalised by Michigan in 1993 through Michigan Criminal Code. The term 'cyber staking' is still not defined by any particular legal provision in the UK. Provisions including Ss.2-7 of the Protection from Harassment Act (PHA), 1987[10] are presently used as the regulatory provision for stalking and cyber stalking.

No legal definition of stalking or cyber stalking was recognized in India before January 2013. Before January 2013 there was no recognised legal definition of stalking or cyber stalking in India. The concept of cyber stalking neither received any new academic understanding in India until 2010, when Halder and Jaishankar provided a functional definition of cyber stalking which is as follows: *"In one word, when 'following' is added by mens rea to commit harm and it is successfully digitally carried out, we can say cyber stalking has happened"*[11].

Stalking was legally recognised as an offence in India through Section 354D of the Indian Penal Code which was inserted through the Criminal Law Amendment Act, 2013. The provision defined stalking in the following words: *"Any man who follows a woman or contacts or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman or whoever monitors the use by a woman of the internet, email or any other form of electronic communication or watches or spies a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such woman or interferes with the mental peace of such woman, commits the offence of stalking".*

The above-mentioned law have been clearly drawn up as a "feminine-centred statute," and the language of the law has placed considerable emphasis on the infringement of privacy in a way that tracks and stalks fear of abuse, grave alarm or distress. It therefore provides a three dimensional explanation to stalking: (i) despite her disinterest, physically persuading a woman repeatedly by conducting in such a way that may create fear in her, may interfere with her peace of mind, (ii) monitoring her digital whereabouts, communications, etc. by digital conducts which create serious threat, alarm or interfere with her mental peace, and (iii) spying or watching her to in order to pose a harm to her[12]. The Act also does not place much focus on

[9] Ellison, L., Akdeniz, Y., *Cyber-stalking: The Regulation of Harassment on the Internet*, Crim. Law Rev, 29-48 (1998).
[10] See the provisions related to harassment in the Protection from Harassment Act, 1987.
[11] Halder, D., Jaishankar, K., *Cyber Victimization in India: A Baseline Survey Report*, CENTRE FOR CYBER VICTIM COUNSELLING, https://www.cybervictims.org/CCVCresearchreport2010.pdf , Last accessed on Apr.08, 2020, 2.32 PM).
[12] Debarati Halder, *Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives*, TEMIDA 103-130 (2015).

 [ISSN 2581-5369]

harassing communications, which are often known as stalking actions by other legal experts, as opposed to current cyber stalking laws in other jurisdictions, such as the USA.

Thus it can be inferred from the above definitions which are both academic as well as legal that cyber stalking as digitally conducted harassment which could inevitably infringe the victim's privacy. The legal concepts of cyber stalking discussed above derive from legislation intended for physical stalking from their conceptualisations.

Before explaining the topic in detail, it is necessary to understand the basic terminology used in this paper i.e, Cyber Space. The term "cyber space" means the environment where the internet is used for communication[13]. In other words, it is a world created by internet. Cyber space can be defined as follows: "a global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers[14]". Another definition is "the virtual space in which the electronic data of worldwide PCs circulate[15]". This is a vague description of cyber space. The main characteristic of cyberspace is that it is composed of various computer networks, switches, routers, servers, etc[16]. It is a cluster of various infrastructures such as transportation, banking, finance, telecommunication, energy and public health[17].

III. Different Manners Of Cyber Stalking:

There are three primary ways in which cyber stalking is conducted:

i. E-mail Stalking: Direct Communication through E-mail.

ii. Internet Staking: Global communication through the Internet.

iii. Computer Stalking: Unauthorized control over another person's computer[18].

E-mail Stalking:

E-mail Stalking is one of the most popular types of stalking in the virtual world, including telephoning, transmitting mail and actual surveillance. One of the most popular forms of harassment is unsolicited e-mail, like hatred, pornographic, or threatening mail. Many other types of harassment include delivering target viruses or online junk mail in large amounts. It is important to remember here that sending viruses or solicitations for telemarketing alone is

[13] *Supra* Note 5.
[14] Defined by U.S. Dept. of Defense.
[15] Defined by European Commission.
[16] *Supra* Note 5.
[17] *Id.*
[18] Anju Thapa, Dr. Raj Kumar, *Cyber Stalking: Crime and Challenge at Cyber Space*, 4 Int. J. Eng. Sci., 340, 342-344 (2011).

 [ISSN 2581-5369]

not a harassment. Nevertheless, if such messages are sent regularly in a way that is meant to intimidate, then they may constitute concerning behaviours which can be categorized as stalking[19].

Internet Stalking:

In the case of internet stalking, stalkers can comprehensively use the Internet in order to slander and endanger their victims. In such situations, the cyber stalking takes on a public dimension instead of a private dimension. The most disturbing thing about this cyber stalking type is the fact that it seems to spill into physical space the most[20].

Computer Stalking:

The third mode is cyber stalking that takes advantage of the Internet and the Windows operating system to gain control of the target's device. It is probably not widely recognized that an individual Windows based computer connected to the Internet can be identified and connected to another computer through to the Internet[21]. This connection is not the link via a third party characterizing typical Internet interactions, rather it is a computer-to computer connection allowing the interloper to exercise control over the computer of the target[22]. A cyber stalker often interacts with their target directly as soon as the target device connects to the Internet in some way. The stalker can assume control of the victim's computer and the only defensive option for the victim is to disconnect and relinquish their current Internet address[23].The circumstance is like finding that a stalker is on-line and in charge of your phone at any time you pick up the phone. The only way to stop the stalker is to completely disconnect the line, and then reconnect with a completely new number. *Only one specific example of this technique was used in stalking for instance, a woman received a message stating "I am going to get you", the interloper then opened the women's CD-Rom drive in order to prove he had control of her computer[24]*. More recent versions of this technology claim to enable real-time keystroke logging and view the computer desktop in real time. It is not difficult to hypothesize that such mechanisms would appear as highly desirable tools of control and surveillance for those engaging in cyber stalking[25].

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*

 [ISSN 2581-5369]

IV. CYBER STALKING V. OFFLINE STALKING:

Cyber stalking is basically an extension of traditional stalking, where the offender uses high-tech modus operandi to commit the crime[26]. With cyber stalking becoming a growing criminological concern in contemporary society, the offender's behaviours and actions need to be examined in greater depth[27]. Cyber-stalking activities in many ways resemble typical stalking behaviours; however, cyber stalking, at least from a criminological and legal perspective, represents an entirely new form of deviant, criminal behaviour. For one, both conventional and online types of criminals turn to strategies and actions specifically intended to annoy and, in some cases, threaten or intimidate the victim[28]. As described above, traditional stalkers and cyber stalkers often respond aggressively when a victim is approached, scorned, ignored or belittled[29].

As repeatedly mentioned, many of the behaviours exhibited by cyber stalkers approximate those of conventional stalkers, but there are many notable differences that clearly distinguish the former from the latter. One of the most striking similarities is that both offender types are motivated by an insatiable desire and need to have power, control, and influence over the victim[30].If left unattended, these acts may potentially escalate into a potentially volatile physical confrontation between the suspect and the victim, even though many, including those in law enforcement, view cyber stalking as relatively harmless[31]. Traditional stalking behaviours are fairly predictable in that the offender will often follow the victim home, to work, or even to school, thereby making it somewhat effortless for investigators to track, apprehend, arrest, and subsequently prosecute the offender[32].

In addition, many stalkers resort to unwanted written messages at the victim's home or office and, in some situations, the perpetrator may make offensive phone calls aimed at inducing the victim's fear and intimidation, both of which can be fairly easily tracked back to the perpetrator[33]. As stated, the above offenses usually leave behind physical evidence to establish a criminal case against the suspect. Another notable distinction between the stalker and the

[26]Petherick W., *Cyber Stalking*, CRIME LIBRARY (May.9, 2007, 10:04 AM), http://www.crimelibrary.com/criminology/cyberstalking

[27] Desai, M., & Jaishankar, K., *Cyber stalking victimization of girl students: An empirical study* 1-23 (Feb. 07, 2007, 9:05 PM).

[28] Petrocelli, J., Cyber *stalking. Law & Order*, 53(12), 56-58 (2005).

[29] Bocij, P., *Reactive stalking: A new perspective on victimization*, 7 The British Journal of Forensic Practice, 7(1), 23-45. (2005).

[30] Reno, J., *1999 Report on Cyber Stalking: A New Challenge for Law Enforcement and Industry*, UNITED STATES DEPARTMENT OF JUSTICE (Feb.18, 2006, 11:05 AM), http://www.usdoj.gov/criminal/cybercrime/cyberstalking.html.

[31] *Id.*

[32] Id.

[33] *Id.*

cyber stalker is the distinctly high likelihood that both types of perpetrator have a previous, actual or imagined, intimate relationship with the victim; however, the cyber stalker is more likely to randomly select his or her victims[34].

Thus to sum up cyber stalking is an online threat and the victim and cyber stalker are not directly related but whereas offline stalking is direct physical threat to the victim and there is some relationship between the victim and the stalker. Cyber Stalking is universal whereas offline stalking is particular. Also there is no prior clear identity about cyber stalker but clear identification is found about the offline stalker. Direct psychical threat can be seen in offline stalking whereas in cyber stalking there is more use of obscene language and verbal intimidation. Enforcement of law is difficult in cyber stalking as it requires sometimes extradition but whereas enforcement of law is easier in offline stalking.

Based on the above differences, a number of criminologists have advised that a solution to cyber stalking is not to use regulations to identify the guilt and ultimately pronounce punishment for physical stalking, but to create a new system for cyber stalkers protection[35]. This new regime should encompass the two basic feature of crime i.e, *actus reus* and *mens rea*. This new system must deal in addressing the issues of identification of crime, gathering evidence and the issues regarding jurisdiction[36].

V. INDIAN LEGISLATIVE FRAMEWORK AND THE DRAWBACKS CONCERNED TO IT:

In this chapter, the main focus has been laid down on the provisions of Information Technology Act, 2000 and Indian Penal Code, 1860 with respect to Cyber stalking. In the Indian Penal Code, the protection has been afforded to women only from the act of stalking thereby making the law of stalking as gender biased. However, this chapter tries to explain few sections of Information Technology Act and Indian Penal Code that have some link with this offence and the explanation has been given regarding the relation between the provisions and the crime.

Some of the provisions of Indian Penal code with respect to cyberstalking as follows:

Firstly, Section 354D of IPC defines "stalking". It reads as follows:

(1) *Any man who-*

i. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

[34] *Supra* Note 28.
[35] *Supra* Note 5.
[36] KW Seto, *How Should Legislation Deal with Children as the Victims and Perpetrators of Cyberstalking?* 9 CARDOZO WOMEN"S L. J. 67, 73-74 (2002).

 [ISSN 2581-5369]

ii. monitors the use by a woman of the internet, email or any other form of electronic communication commits the offence of stalking.

Provided that such conduct shall not amount to stalking if the man who pursued it proves that-

i. It was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or

ii. It was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

iii. in the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine[37].

The aforesaid section was added through the Criminal Amendment Act 2013 after the Delhi gang rape case in order to uplift the women in the society and for protecting them against all forms of sexual harassment faced by them. The said section takes into account both the physical stalking and cyber stalking. There is an explanation of the activities that forms the offence of "stalking". It is clearly mentioned that if anyone tries to monitor the activities of a woman on internet, it will amount to stalking. Thus, if the stalker indulges in any of the activities defined in the section, he shall be guilty of the offence under Section 354D of Indian Penal Code.

This section has many loopholes such as firstly; the section only considers "women" to be the victim and ignores the fact that even men can be the victim. The Section states that whoever tries to monitor the usage by a woman of internet, e-mail or any other mode of electronic communication shall be liable for committing the offence of cyber stalking. We can see that it focuses only on women. Thus, it is gender biased legislation. Secondly, the legislators have not mentioned the "method of monitoring." It might happen that the person might lack the intention but his actions amount to stalking[38].

Secondly, Section 292 of IPC defines "obscenity". The offence of cyberstalking takes within its purview the act of sending obscene materials to the victim on a social networking site or through emails or messages etc. Where the stalker attempts to deprave the other person by sending any obscene material on internet with the intention that the other person would read,

[37] Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860.
[38] *Supra* Note 5.

 [ISSN 2581-5369]

see or hear the content of such material then he shall be guilty of the offense under Section 292 of Indian Penal Code.

Thirdly, Section 507 of IPC relates to "criminal intimidation by anonymous communication." This section states that where the stalker tries to hide his identity so that the victim remains unaware of the source from where the threat comes, it amounts to an offence. Thus, it ensures the very characteristic of cyberstalking i.e., anonymous identity. The stalker shall be guilty under this section if he attempts to conceal his/her identity[39].

Fourthly, Section 509 of IPC relates to modesty of women reads as follows:

"Word, gesture or act intended to insult the modesty of a woman.—Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished..."[40]

A stalker can be held liable under this section if the stalker's behaviour hinders the woman's privacy by making some gesture or by using words sent through e-mails, texts or shared on social media. If he does any such activities, he shall be guilty of offence under Section 509 of Indian Penal Code.

Some of the loopholes of Section 509 is that it is a gender biased provision as it focuses only on modesty of a woman and therefore, ignores the fact that this crime of cyberstalking is gender neutral in nature and even males can also be the victim in such crimes. This section requires that the words, sound or gesture should be spoken, heard and seen respectively. Thus, cyber-stalkers can easily escape the penalty under this section as word cannot be spoken, gesture cannot be seen and sound cannot be heard on internet.[41] Lastly, the purpose of undermining the woman's modesty can't be inferred from internet communications.

Some of the provisions of Information Technology Act, 2000 with respect to Cyber stalking are:

Firstly, Section 67 of Information Technology Act, 2000 is replica of Section 292 of Indian Penal Code. This section relates to publishing obscene material in "electronic form". Thus, this section covers the online stalking. If the stalker tries to publish any obscene material about the victim on social media i.e., in electronic form so as to bully the victim, he shall be guilty of offence under Section 67 of IT Act.

[39] *Id.*
[40] Indian penal Code, 1860, No.45, Acts of Parliament, 1860.
[41] P. Duggal, *India's first Cyberstalking Case- Some Cyber law Perspectives*, MANUPATRA (May 13, 2017, 8:55 PM), http://cyberlaws.net/cyberindia/2CYBER27.html.

 [ISSN 2581-5369]

Secondly, Section 67A of Information Technology Act, 2000 relates to a part of cyberstalking crime. This section was added after the amendment in 2008. It states that if stalker attempts to publish any "sexually explicit" material in electronic form i.e., through emails, messages or on social media then he shall be guilty of an offence under Section 67A of IT Act and shall be punished accordingly.

Thirdly, Section 67B of Information Technology Act, 2000 is a newly inserted section. This section is newly inserted by Amendment Act 2008. The section focuses on when stalker targets children below the age of 18 years and publishes material in which children are engaged in sexual activities in order to terrorize the children.

Fourthly, Section 66E of Information Technology Act, 2000 and Section 354C of Indian Penal Code deals with "voyeurism." Section 66E reads as follows:

"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished."[42]

Fifthly, Section 354C reads as follows:

"Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished…"[43]

In order to induce depression and a sense of fear in the mind of the victim, the stalker might access the victim's account and place private photos on social networking sites. Both the above-mentioned sections aim at publishing or capturing pictures of private act of a person without the consent of such person shall be guilty of an offence under these sections[44]. However, Section 66E is more generic as it addresses the victim as "any person" whereas Section 345C is kind of gender biased. As per section 354C, the victim should be a "woman".

"What is noteworthy here is that despite the fact that all offline laws apply to digital media, the punishments under the IT Act are much stronger."[45] "Indeed, it is worth noting the emphasis placed even by the IT Act on women's bodies or sexualities: within the Act, while Section 66A

[42] Information Technology Act, 2000, No. 21, Act of Parliament, 2000.
[43] Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.
[44] *Supra* Note 5.
[45] Richa Kaul Padte, *Keeping woman safe? Gender, Online Harassment and Indian Law*, INTERNET DEMOCRACY PROJECT (Jun. 29, 2013, 8:45 AM), https://internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law/

 [ISSN 2581-5369]

deals with a generic category of 'offensive messages'[46].

Section 354C of Indian Penal Code takes within its purview the act of voyeurism. It is comparatively narrow in scope because to attract this section, the victim should a "woman". On the other hand, Section 66E of Information Technology Act also covers voyeurism but the scope is broader as compared to Section 354C of Indian Penal Code. Section 66E addresses the victim as "any person". Thus, the victim need not be only "woman" in order to fetch justice under this section. Where the victim is a man, he may take recourse to Section 66E of Information Technology Act, 2000.[47]

There is no express provision regarding the cyber stalking and the defamatory or threatening messages sent by the stalker during stalking the victim through messages, phone calls, e-mails or by publishing blogs under the name of the victim under Information Technology Act, 2000 and the Indian Penal Code, 1860. In accordance with the provisions of the above-noted Acts, the perpetrator may be punished as stated above, but no particular provision is given for dealing with this crime alone[48]. It is very quick to commit this crime, although its consequences are very prolonged. Mental and physical wellbeing can be seriously affected by this. The punishment under the present provisions must be increased taking the protection of the victim into account[49].

VI. The Problem Of Enforcement In The Context Of Indian Constitutional Framework:

In the Information Technology Act, 2000 or the Information Technology Amendment Act, 2008, the principal question of territorial authority has not been addressed effectively. The different sections in which the question of jurisdiction has been mentioned are Sections 46, 48, 57 and 61, where the method of adjudication and the appeal procedure are listed. Another section is Section 80 which describes the powers of police officers to enter and undertake search in a public place in relation to a cyber-crime etc. The cyber-crimes are the crimes that are committed with the help of computers and if someone hacks the mail account of a person sitting in another state or country, it will be difficult to determine P.S. of which shall take the cognizance of the offence.

Many police officers tend to stop admitting the victim's allegations because of the jurisdiction problem in these situations. Since the cybercrimes are not bound by the territorial boundaries,

[46] *Id.*
[47] *Supra* Note 5.
[48] *Id.*
[49] Vijay Mukhi and Karan Gokani, Observations on the Proposed Amendments to the IT Act 2000, AIAI.

 [ISSN 2581-5369]

the question of jurisdiction needs to be explained as what all the relevant criteria are to be seen in these circumstances[50]. Proper elaborations should be made as to which State has the authority to deal with the cybercrime cases.

The solution to the problem can be the extradition arrangement between the two respective countries. An extradition arrangement is an arrangement where the criminal is deported to the country where he has committed the crime in case where such arrangement exists between the two concerned countries[51]. So as in the case of cyber stalking, if there is an agreement between the country to which the victim belongs and the country to which the stalker belongs, then no such enforcement issue will occur[52].

Jurisdictional issues arise when one law of the country is not in conformity with the laws of the other country. A stalker may be penalized in one country but may not be regarded as a crime in another country. In such situation the problem of enforcement arises and the cooperation and extradition policies between the countries comes into role play. Section 75 of the Information Technology Act provides for the 'extraterritorial jurisdiction' in India. This section makes it clear that whether an offence is committed outside or in India, the offender shall be governed by the provisions of Information Technology Act irrespective of the fact whether he is a citizen of India or not. Provided such an offence relates to the computer systems, or network that is situated in India. Thus, the solution provided by Indian laws to the problem of enforcement is limited.

One of the traits of cyber stalking is the stalker's anonymous identity. There has been suggestion to limit the anonymity of identification. However, this seemed to be a debatable issue since virtually every country's law guarantees freedom of speech and it would breach this right to limit anonymous identity. In the cases of *In Re RamlilaMaidan Incident* v. *Home Secretary*[53] and *Sahara India Real Estate Corp. Ltd*. v. *Securities & Exchange Board of India*[54], the court held that the freedom of speech and expression as provided under Article 19(1)(a) is not an absolute right.

After 2013, society has been changing and law being dynamic in nature should be changed now and then so that objectives of providing security to people and ensuring law and order can be achieved. It is accepted that 2013 Criminal Amendment was brought to protect the women against sexual exploitation but now the time has changed and the women are using these laws

[50] *Supra* Note 5.
[51] *Id.*
[52] *Id.*
[53] (2012) 5 SCC 1.
[54] (2013) 1 SCC 1.

 [ISSN 2581-5369]

which are in favour of them as tool to file false complaints against men. It has to be noted that men are also the victim of stalking and such cases are increasing rapidly. Section 354D of Indian Penal Code is prominent law on stalking which itself prima facie a gender biased law and this lacunae has to be addressed otherwise the concept of equality enshrined under Article 14 of the Indian constitution cannot be embodied in the said provision of IPC and the objective of treating equally cannot be achieved. Thus the terms "man" and "woman" should not be explicitly used. The section should be reframed using the term "anyone" or "any person" to make it non-violative of Article 14.

The issue of a woman's modesty is discussed under section 509 of the Indian Penal Code. This section should also be reframed by the term "any person" instead of "woman". A female stalker can also offend the modesty of a man through sending obscene materials on internet or e-mails or messages, the stalker. Thus it is the need of the hour that legislators should make an attempt to protect man and woman and not just the woman both from the ill-effects of cyber stalking. Section 354C of Indian Penal Code deals with voyeurism which also a part of cyber stalking as the offender/stalker might indulge in hacking the computer of the victim so as to have a look on to the private pictures of the victim without his/her consent. This section is also gender biased and same has to be addressed.

VII. Conclusion And Suggestions:

Cyber stalking is a newly coined term. This has been considered as offence considering the grave intensity of the said offence as it affects the both mental as well physical health of the victim. This offence has attracted the attention of legislature and judiciary and need has been felt for the effective legislation and enforcement agencies to deal with such cases. Arguments have been laid down contending that cyber stalking is an extended version of stalking but it is a new crime itself. In the said offence, the main intention of the stalker is to harass or threaten his/her victim. Thus, it involves a criminal activity. Many countries even have specific legislations on the said subject. India lacks such specific legislation and the current provisions dealing either directly or indirectly are inefficient in reducing such offences because of the enforcement problems that are pointed out in this paper. There are hardly any reported cases because the police authorities do not take up the case because of the enforcement issues as the stalker and the victim may belong to different countries thus, it becomes difficult to decide as to law of which country is to be followed. Thus legislature should consider the said complexities in already passed law and come up with an efficient legislative framework to deal with these serious kind of offences.

Some of the suggestive reforms are as follows:

 [ISSN 2581-5369]

1. The law relating to stalking incorporated under Section 354D of Indian Penal Code should be gender neutral law. The terms "man" and "woman" should not be explicitly used. The section should be reframed using the term "anyone" or "any person."

2. Section 66A of Information Technology Act was added in the year 2008 to address the issue of cyber stalking but was eventually struck down by the Supreme Court of India in the case of *Shreya Singhal v. Union of India*[55].Considering the vagueness in the aforesaid section, it was been striked off in the above-mentioned case. And the present provisions of information technology act do not address the issue of cyber stalking directly, henceforth there is a need for the amendment of the Act. A new section has to be added to the information technology act solely dealing with cyber stalking. The said section should define the offence, include all forms of medium usage done for the act of stalking prescribe severe punishment. However, it has to be noted that by making such an amendment, the offence of cyber stalking could be reduced to much extent as there will be rigorous imprisonment provided under the said amendment if found guilty. It makes it an offence to keep anonymous identity and covers almost every mode of electronic communication or computer resource using which the stalker tries to communicate with the victim.

3. Thirdly it is important that people must try to protect themselves from becoming the victim of these cyber crimes. Self-regulation is most efficient method to control such crimes. Less number of personal information should be disclosed on social networking websites. Photos and other privacy settings must be done and protected. The passwords must be combination of words, characters and numbers and must be of strong nature so that the account wont be easily hacked. Personal information should not be shared easily when having communication with the strangers. Government must ensure that proper awareness must be created among people on how to use internet and what precautions must be taken while interacting with strangers on social networking sites. For example, Government initiative is the collaboration between the U.S. Department of Justice in collaboration and the Information Technology Association of America declared their Cybercitizen Partnership in 1999. This collaboration was intended to spread awareness about crimes related to computers.

4. To limit the stalker's harassing behaviour, Internet Service Provider has taken few steps. Few providers provide the opportunity to report abuses for example, Facebook as discussed above, Facebook has certain privacy policies whereby we can restrict strangers from sending

[55] AIR 2015 SC 1523.

 [ISSN 2581-5369]

messages containing obscene content and abusive behaviour. Internet Service Providers take control measures by sending unwanted emails to spam folder. For the successful curbing of these cyber-crimes it is necessary that there must be a cooperation between Internet Service Providers and the enforcement agencies when it comes to tracking down the stalker.

Thus the results can be seen over a period of time if the aforesaid measures with other any efficient measures so shall be adopted can help for curbing these type of cybercrimes at faster pace. Effective legislative provisions is the need of the hour and the same must be successfully implemented.

*****

 [ISSN 2581-5369]