GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

LEGISLATIVE AND JUDICIAL RESPONSES TO CYBER STALKING AGAINST WOMEN: AN INDIAN PERSPECTIVE

Neha K. Bhatt, Dr. Pareshkumar D. Dobariya

Pursuing Ph.D. in Law.

Assistant Professor, Smt. V.D. Gardi Law College, Wadhwan, Dist. Surendranagar, Gujarat.

"Give light and the Darkness will disappear itself"

-Desiderious Erasmus[1]

Abstract

Cyber Crime is the dark side of digital technology. Cyber Stalking is one of the cybercrimes against Individual which has been continuously growing in Digital era. The Cases of cyberstalking or bullying of women or children increased by 36% from 542 in 2017 to 739 in 2018, data released recently by the NCRB showed. Meanwhile, the conviction rate for cyberstalking or bullying of women and children fell 15% points, to 25% in 2018 from 40% in 2017.[2]Despite Information Technology Act 2000 and other legislations Cyberstalking crime is on the rise in India. Despite these prevailing situations, the Indian judiciary is still a ray of hope. To curbing this digital crime we need to throw light on present Cyber Stalking crime's situations and do amendments in current prevailing cyber legislations in India. Through this paper, the researcher will try to study Cyber Stalking against women in India. This paper is an attempt to analyze the Indian legislation, Cyber Legislation for Cyber Stalking, and the Judiciary's approach relating to the rights of women in cyberspace upholding Gender Justice.

***Key Words**: Digital Technology, Cybercrime, Cyberstalking, Cyber Legislation, Indian Judiciary.*

INTRODUCTION

At present time its rapid growth of Information Technology is enclosing all walk of life. These technical improvements have transformed documents to paperless communication possible. The wide extension of Internet and Computer technology globally has led to the escalation of internet-related crimes. In the Asia region, India has ranked the top two internet user countries. India has become a major spot for cybercriminals. India is ranked fifth in cybercrime amongst other countries.[3] Cyberspace is being taken up by a new form of crime that includes a repetitive attempt by one person to contact another thereby causing a sense of threat in the mind of such other person. This emerging crime is popularly known as "Cyber Stalking". It involves the conduct of harassing or threatening repeatedly to an individual. Stalking can be done in the following ways such as: to follow a person to his home or where he does his business, to destroy a person's property, leaving written messages or objects, or making harassing phone calls. Cyber stalkers always think that they're anonymous and can hide. In other words, the cyber stalker's biggest strength is that they can rely upon the anonymity which internet provides to them that allows them to keep a check on the activities of their victim without their identity being detected. Thus, there is a need for efficient cyber tools to investigate cybercrimes and to be prepared to defend against them and to bring victims to justice.[4]

DEFINITIONS

Introduction:

The dictionary meaning of the adjective 'Stalking' means "of or relating to the act of pursuing or harassing". The word stalking was not commonly known until various instances happened. The legal definition of stalking varies from country to country. Various definitions are available in several books, out of which it can be stated that the common elements are; repeated and unwanted behaviour whereby one individual attempts to contact another

[1] Available at http://ujala.uk.gov.in/files/ch20.pdf (Accessed on 24th May 2020 at 11:36 pm).
[2] Available at. https://scroll.in/article/956085/in-one-year-alone-cyberbullying-of-indian-women-and-teenagers-rose-by-36 (Accessed on 8th June 2020 at 10:44 pm).
[3] Nidhi Arya, "Cyber Crime Scenario in India and Judicial Response" Pub. By (ijtsrd), ISSN: 2456-6470, Volume-3 Issue-4, June 2019, pp.1108-1112, URL: https://www.ijtsrd.com/papers/ijtsrd24025.pdf.
[4] Ms. Heena Keshvani, Cyber Stalking: A Critical Study pub. By Bharati Law review, April – June 2017, pp.131 available at http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf (Accessed on 9th June 2020 at 07:10 pm).

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

individual, and the behaviour causes the victim to feel threatened or harassed.[5] Women and Children are mostly soft targeted.

Cyberstalking:

The phenomenon of stalking emerged in the USA in the 80s. In the beginning, it concerned people who would be constantly monitored by the media due to their popularity. Stars also became victims of their own fame because of their fans obsession, they would be followed and harasses in various ways.[6] Cyber-stalking refers to stalking activities conducted in 'cyberspace' using information and communication technologies. Cyber-stalkers may utilize a range of tools and virtual environments including email, chat rooms, bulletin boards, newsgroups, instant messaging, and key-logging Trojans. In their study of New York Police Department cyber-stalking cases, D'Ovidio and Doyle (2003) reported the most commonly used methods of cyber-stalking were email (79%) and instant messages (13%). As with stalking in general, there is no consistently used definition of cyber-stalking in the literature. It should be noted however that the term cyber-stalking is itself not accepted universally. For example, Bahm (2003) argues in favour of the terminology 'the use of technology to stalk' to cover current and future forms of technology that can be used in stalking.[7]

There have been several attempts by experts and academicians to define cyberstalking. It is generally understood to be the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. Cyberstalking is a form of cyberbullying; the terms are often used interchangeably in the media. Both may include false accusations, defamation, slander, and libel. Cyberstalking may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass. Cyberstalking is often accompanied by real time or offline stalking. Both forms of stalking may be criminal offenses. Stalking is a continuous process, consisting of a series of actions, each of which may be entirely legal in itself.[8] So many experts have tried their level best to define these "Cyber Stalking" terms which are mention below.

- **British Crime Survey** has tried to define Cyber Stalking. "Cyberstalking is a criminal practice whereby a person uses the internet, cell phone, and/or any other electronic communication device to stalk another person." The perpetrators are involved in the destruction of data or equipment, solicitation of minors for sexual purposes, threats, or any other form of offensive behaviour committed repeatedly. The offenders make use of email, social media, chat rooms, instant messaging, or any other online media to harass the victim.[9]
- **According to Bocij and McFarlane:** Another detailed definition of Cyber Stalking that includes organizations by Bocij and McFarlane (2002) is A group of behaviours in which an individual, group of individuals or organization, uses information and communications technology (ICT) 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 intimidation purposes, and confrontation. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress. This definition shows cyberstalking may sometimes involve harassment carried out by an organization also. Such behaviour is often termed corporate cyberstalking.[10]
- **According to Indian Penal Code 1860:** Section: 354D was added by the Criminal Amendment Act 2013 and it covers both kinds of physical stalking and cyberstalking. Section 354D of IPC defines "stalking". It reads as follows:

"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 (ii) monitors the use by a woman of the internet, email or any other form of electronic communication commits the offense of stalking;.."[11]

This section is exclusively focused on women netizens and give protection. It is not given protection to men victims. Secondly, the legislators have not mentioned the "method of monitoring." The person might lack the

[5] Dr.Mrs.Hema.V.Menon, Cyber Stalking In The Indian Scenario And The Indian Information Technology Act, 2008., Aayushi International Interdisciplinary Research Journal (AIIRJ)Vol-III Issue-I January 2016 ISSN 2349-638x Impact Factor 2.147 available at https://www.aiirjournal.com/uploads/Articles/2016/01/307_04.Dr.Menon%20H.V..pdf(Accessed on 28th July 2020 at 11:39 am).

[6] Chahal, Rohini, Kumar, Lovish, Jindal, Shivamand Rawat, Poonam (2019). Cyber Stalking: Technological Form of Sexual Harassment. International Journal on Emerging Technologies, 10(4): 367–373, available at https://www.researchtrend.net/ijet/pdf/Cyber%20Stalking%20Technological%20Form%20of%20Sexual%20Harassment%20Shivam%20Jindal.pdf (Accessed on 5th August 2020 at 03:51 pm).

[7] Lynne Roberts, Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking, International Journal of Cyber Criminology Vol 2 Issue 1 January 2008 available at http://www.cybercrimejournal.com/lynnerobertsijccjan2008.pdf (Accessed on 22nd July 2020 at 01:50 pm).

[8] Cyberstalking, available at https://en.wikipedia.org/wiki/Cyberstalking (Retrieved on 17th July 2020 at 05:24 pm).

[9] Available at https://blog.ipleaders.in/cyber-stalking/(Accessed on 5th August 2020 at 06:40 pm).

[10] Available at https://www.researchgate.net/profile/Alok_Mishra5/publication/287557261_Cyber_stalking_A_challenge_for_web_security/links/5a83e26c45851504fb3a8ec1/Cyber-stalking-A-challenge-for-web-security.pdf (Accessed on 14th August 2020 at 12:43 pm).

[11] Section 354D of Indian Penal Code 1860 (Act No.45 of 1860).

intention but his actions amount to stalking.[12] This section has one more lacuna that it has not given clarity about "Monitoring Method". Cyber stalkers might terrorize victims by sending unpleasant messages systematically, perhaps even several times a day. It is especially unnerving when such messages come from different accounts managed by the same person. It is probably a good idea to report this to both the website owners and law enforcement agencies. Cyberstalking doesn't have to involve direct communication, and some victims may not even realize they are being stalked online. Perpetrators can monitor victims through various methods and use the information gathered for crimes like identity theft. In some cases, the line between cyberspace and real-life can become blurred. Attackers can collect your data, contact your friends and attempt to harass you offline.[13]
In the US laws, cyberstalking was considered as "harassment". Presently many provinces of the US have enacted anti cyberstalking laws, which explained cyberstalking in a similar connotation as harassment. The term 'cyber stalking' is still not defined by any particular legal provision for stalking and cyberstalking in the United Kingdom. Provisions including Ss.2-7 of the Protection from Harassment Act (PHA), 1987 are presently used as the regulatory provision for stalking and cyberstalking. In India, there were no cyberstalking laws until 2013. There were huge confusions regarding what constitutes cyberstalking. In 2013, vide Criminal Law Amendment Act, 2013, the Indian Government introduced anti-stalking law (covering cyberstalking as well) through S.354D, IPC whereby these two stages of cyberstalking were introduced. [14] Typically, the cyber stalker's victim is new on the Web and inexperienced with the rules of netiquette and Internet safety. Their targets are mostly females, children, emotionally weak, or unstable persons. It is believed that over 75% of the victims are female, but sometimes men are also stalked.[15] According to Baum et al. (2009), roughly stalking victims reported some form of cyberstalking, such as e-mail (83%) or instant messaging (35%), while electronic monitoring and Global Positioning System (GPS) technology were used in several cases. The criminal phenomenon of cyberstalking is difficult to quantify; as King-Ries (2011) remarks, data on cyberstalking is still in its infancy. As cyberstalking can have a very negative impact on victims, resulting in anxiety or fear and loss of trust in people, it needs to be effectively addressed by stakeholders.[16]

DIFFERENCE BETWEEN CYBER STALKING AND PHYSICAL STALKING

To discuss the difference between cyberstalking and physical stalking, there is a need to understand what does physical stalking mean and includes acts which are intended towards harassing the victim. The difference between these two are as follows[17]:

- **Physical Stalking** is committed when a person intentionally and for no legitimate purpose, engages in a course of conduct directed at a specific person, and knows or reasonably should know that such conduct is likely to cause fear of material harm to the physical, mental, or emotional health, safety or property of such person, a member of such person's immediate family or a third party with whom he or she is acquainted. It could be included that this act creates a reasonable fear of a person's employment, business, or career place. This is typically accomplished by following someone or appearing at their home, school, or place of business, making harassing phone calls, leaving messages or objects, or vandalizing the person's property. In physical stalking, there is a direct relation between victim and stalker. Geographical proximity is in this kind of stalking so enforcement of the law could be easy in it. It is very dangerous for the victim as a stalker knowing the victim very well. In physical stalking, the victim can easily identify the fake intentions of the stalker. Compare to Cyberstalking there is a high degree of risk for the victim in physical stalking.
- **Cyber Stalking** is similar behaviour through the use of the internet or other electronic means to accomplish the same end. The fact that cyberstalking doesn't involve physical contact doesn't mean that it is less dangerous than physical stalking. An experienced Internet user can easily find the victim's personal information such as phone number, address, or place of business to locate their whereabouts. This can be then lead to more

[12] Ms. Heena Keswani (2017), CYBER STALKING: A CRITICAL STUDY, Bharti Law Review April-June (2017) available at http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf (Accessed on 17th July 2020 at 06:06 pm).
[13] Available at https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/ (Accessed on 5th August 2020 at 07:55 pm).
[14] Debrati Halder & K. Jaishankar (2017), Cyber Crimes against Women in India, Sage Pub. India Pvt Ltd ISBN: 978-93-859-8577-5 (HB) page no. 98-100.
[15] Available at https://www.researchgate.net/profile/Alok_Mishra5/publication/287557261_Cyber_stalking_A_challenge_for_web_security/links/5a83e26c45851504fb3a8ec1/Cyber-stalking-A-challenge-for-web-security.pdf (Accessed on 14th August 2020 at 12:53 pm).
[16]Loana Vasiu & Lucian Vasiu (October 2013), Cyberstalking Nature &Response Recommendations, AJOIS Vol.2, No.9 Oct.2013 E-ISSN 2281-4612, Mcser Pub. Rome Italy is available at https://www.researchgate.net/publication/271040560_Cyberstalking_Nature_and_Response_Recommendations (Accessed on 20th August 2020 at 09:42 pm).
[17] Ms. Heena Keswani (2017), CYBER STALKING: A CRITICAL STUDY, Bharti Law Review April-June (2017) available at http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf (Accessed on 8th September 2020 at 07:37 pm).

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

physical behaviour.[18] This kind of stalking sometimes very difficult to enforce law due to territorial jurisdiction. The Internet provides a feature of ensuring a false sense of closeness between the stalker and the victim. This results in a misunderstanding of the stalker's intention.

Based on the above-mentioned differences, several criminologists have advised that a solution to cyberstalking is not to take recourse to regulations to identify the guilt and eventually pronounce punishment for physical stalking but a new system must be created for protection against cyber-stalkers. This new regime should encompass the two basic features of crime i.e. actus rea and mens rea. This new system must deal in addressing the issues of identification of crime, gathering evidence, and the issues regarding jurisdiction.[19] Comparing to Cyberstalking there is a high degree of risk for the victim in physical stalking.

There are mostly three ways to conduct Cyberstalking. E-mail Stalking, Internet Stalking, and Computer Stalking. E-mail is one of the most common ways of harassment. In Internet Stalking, a stalker can more comprehensively use the Internet to slander and endanger their victims. Computer Stalking: The stalker exploits the working of the internet and the Windows operating system to assume control over the computer of the targeted victim. A cyber stalker can communicate directly with their target as soon as the target computer connects in any way to the Internet.[20]

LEGISLATIVE PROVISIONS FOR CYBERSTALKING IN INDIA

Gender harassment through cyberspace has become a common phenomenon in the internet era (Citron, 2009a). But harassment is worsened when victims face further victimization due to denial of justice at the hands of the criminal justice system. Countries such as the United States, the UK, and India have codified laws dealing with cybercrimes and cyber-harassment to protect the victim. Ironically, the same systems pave the way for secondary victimization.[21]Cyberstalking is a serious crime, a type of offense committed by the person known as a stalker. There are many cases filed against those persons by the victim every year in India. In India the cases which are filed against those stalkers are majorly reported by females, nearly about 60% of females get victimized. The stalking is majorly spotted in the two states of India; Firstly, Maharashtra with 1,399 cases had a higher number of stalking. Secondly, Delhi with around 1130 cases is filed against stalking.[22] Before February 2013, there were no laws that directly regulate cyberstalking in India. India's Information Technology Act of 2000 (IT Act) was a set of laws to regulate cyberspace. However, it merely focused on financial crimes and neglected interpersonal criminal behaviours such as cyberstalking (Behera, 2010; Halder & Jaishankar, 2008; Nappinai, 2010). In 2013, the Indian Parliament made amendments to the Indian Penal Code, introducing cyberstalking as a criminal offense.[23] Cyberstalking is a serious crime worldwide and the number of cases of it goes on increasing every year. In India, a large percentage of cases filed against cyberstalking are by women. The Cyberstalking cases have been dealt with by Information Technology Act 2000 and the criminal law (amendment) act 2013. To deal with cyberstalking in India following provisions of the Information Technology Act 2000 are available:

- **Information Technology Act, 2000**: – When a person publishes or sends salacious material via electronic media is to be charged under Section 67 of the Act. Data protection is very important to prevent cyberstalking which is easily leaked by hackers. For data protection, the IT Amendment Act, Section 43A has been included the provision for the inclusion of a Body Corporate. If a firm or a company transmits sensitive information about a person, according to the act such body corporate will be liable to pay the damages by compensation.
- **Section 67**: Under Section 67 of the Act, when a stalker sends or posts any obscene content to the victim via electronic media then they will be liable to punish with 5 years of jail and Rs. 1 Lacs fine. If the incident repeats then they will be liable to punish with 10 years of jail and a Rs. 2 Lacs fine. As per the provision provided in the law, when a stalker misuses a victim's personal information to post an obscene message or comment on any electronic media, then this action is punishable for defaming and harming a person's reputation with imprisonment of 2 years, fine or both.

[18] Retrieved from http://www.hunter.cuny.edu/publicsafety/policies-and-procedures/stalking-information/stalking-physical-and-cyber-stalking (Accessed on 9th September 2020 at 01:35 pm).

[19] Ms. Heena Keswani (2017), CYBER STALKING: A CRITICAL STUDY, Bharti Law Review April-June (2017) available at http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf (Accessed on 9th September 2020 at 01:51 pm).

[20] Dr. S.R. Myneni (2021), Information Technology Law (Cyber Laws) 2nd Edition Asian Law House Page No. 545.

[21] Debarati Halder & K. Jaishankar, Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India available at https://www.tandfonline.com/doi/citedby/10.1080/15564886.2011.607402?scroll=top&needAccess=true (Accessed on 14th June 2021 at 02:55 pm).

[22] Available at https://taxguru.in/corporate-law/cyber-stalking-cases-cyber-stalking-dealt-indian-court-law.html (Accessed on20th October 2020 at 11:30 pm).

[23] Available at https://en.wikipedia.org/wiki/Cyberstalking_legislation#India (Accessed on 21st October 2020 at 07:15 pm).

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

- **Section 67A**: of the Act which is another provision dealing with cyberstalking and as a replica of Section 292 of Indian Penal Code Section 67A of the Act which is another provision dealing with cyberstalking and as a replica of Section 292 of Indian Penal Code. As this section relates to publishing obscene material in electronic form, it can be related to online stalking. In cases where the stalker publishes any obscene material about the victim in electronic form, he shall be guilty of an offense under Section 67A of the IT Act.
- **Section 66E**: Section 66E of the Act deals with voyeurism and 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 with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both."
- **Section 67B:** Section 67B of the IT Act deals with the publishing of obscene material targeting children below 18 years of age and states that: Punishment for publishing or transmitting of material depicting children in the sexually explicit act, etc. in electronic form. [24]
- **Section 72**: As per this section, Cyberstalking is also covered under the ambit of it and punishable act under this said section. The perpetrator can be booked for breach of confidentiality and privacy.
- **Section 43A:** In 2008 amendment has been made in Information Technology's Act 2000 and amended act. As per Section 43A, Where a body corporate, possessing, dealing, or handling any sensitive personal data or information in a computer resource which it owns, controls, or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation. The Act causes the corporate body to face civil liability under nuisance.[25]

❖ **Indian Penal Code 1860:** To deal with cyber Stalking following sections are available under Indian Penal Code 1860.

- **Section 354C**: Voyeurism is a punishable act under IPC 1860.
- **Section 354D**: The Criminal Law (Amendment) Act, 2013: – According to this provision, Stalking is an offense under Section 354D of the IPC (Indian Penal Code). When a man is trying to communicate with a woman without her interest over the internet via email, instant messages or any other electronic communication is the offense of stalking. Racism is also a kind of cyberstalking.[26] In this provision stalking by email, following by social media, continuous calling phone, and missed calls can be punishable under this provision. Provision must be used and cognizance must be taken when it is a case of 'repeated missed calls' and not just one or two missed calls.[27]
- **Section 499:** The victim can also additionally file a complaint against the perpetrator under Section 499 of IPC which deals with defamation. The section has bailed out those acts of stalking which are performed to prevent and detect crime by a person who has been entrusted with such responsibility by the state. Additionally, instances were pursuing such conduct was reasonable or where the person was authorized under any act cannot insinuate the offense of stalking.
- **Section 503**: Section 503 punishes criminal intimidation as threats made to any person with an injury to her reputation, either to cause alarm to her or to make her change her course of action regarding anything she would otherwise do/not do. The offenses under S. 499 and S. 503 are punishable with imprisonment which may extend to two years, and/or fine. Section 509 of IPC comes to the rescue of a victim when the perpetrator is constantly bugging you with derogatory verbal abuse because of your gender. The section provides that any person who utters any word or makes any sound or gesture, intending that such word, sound, or gesture be heard or seen by a woman and insult her modesty, shall be punished with one-year imprisonment and/or fine.
- **Section 507**: also do punishment to criminal intimidation by an anonymous communication with a term which may extend to two years of imprisonment. Wrongful posting of images or videos of rape victims is punishable with imprisonment which may extend to two years and a fine under section 228a of IPC.[28]
- **Section 509:** Word, Gesture, or act intended to insult the modesty of women is also punishable under such section.
- **Section 11(iv) of the POSCO Act** can be applied if stalking is done as a course of sexual harassment to the girl concerned.[29]

❖ **Jurisdiction:** Territorial limitation on the Internet becomes peripheral in the virtual medium as the web pages on the net can reach almost every province in the nation and conceivably almost every nation on the globe. This is where the point of friction between the cyber world and the territorial world begins as in the

[24] Diksha Bhasin & Aryan Mehta, Cyber Stalking: New Age Terror, IJLMH Volume 2, Issue 1 2019 ISSN: 2581- 5369 available at https://www.ijlmh.com/cyber-stalking-new-age-terror/ (Accessed on 4th December 2020 at 10:13 am).
[25] Available at https://blog.ipleaders.in/cyberstalking-crime-tort/ (Accessed on 24th December 2020 at 06:44 am).
[26] Available at https://vidhisastras.com/cyber-stalking-in-india/ (Accessed on 21st October 2020 at 07:32 pm).
[27] Debrati Halder & K. Jaishankar (2017), Cyber Crimes Against Women In India, Sage Pub. India Pvt Ltd ISBN: 978-93-859-8577-5 (HB) page no.100-101.
[28] Diksha Bhasin & Aryan Mehta, Cyber Stalking: New Age Terror, IJLMH Volume 2, Issue 1 2019 ISSN: 2581- 5369 available at https://www.ijlmh.com/cyber-stalking-new-age-terror/ (Accessed on 4th December 2020 at 10:25 am).
[29] Debrati Halder & K. Jaishankar (2017), Cyber Crimes against Women in India, Sage Pub. India Pvt Ltd ISBN: 978-93-859-8577-5 (HB) page no.101.

territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world. The IT Act will apply to the whole of India unless otherwise mentioned. It applies also to any offense or contravention thereunder committed outside India by any person. However, if a crime is committed on a computer or computer network in India by a person resident outside India, then can the Courts in India try the offense? According to Sec.1 (2) of the Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offense or contravention committed outside India by any person. Further, Sec.75 of the IT Act, 2000 also mentions the applicability of the Act for any offense or contravention committed outside India. According to this section, the Act will apply to an offense or contravention committed outside India by any person, if the act or conduct constituting the offense or contravention involves a computer, computer system, or computer network located in India.[30]

Section 354D is not specifically defined as Cyberstalking. The definition of Cyber Stalking is very narrow and limited compare with the United Kingdom and the United States. S.354D still needs to be analyzed, examined, expanded and amended by the courts. Another loophole of this S.354D is that women-centric law and its bailable offense on a first conviction. It is nonbailable on second conviction. It might be possible that the stalker does again harassment as not rigorous punishment for cyberstalking. This may happen for several reasons, including anonymity to the identity of the stalker, no action by the service provider to monitor the stalker's profile/s, and so on (Halder 2015). In countries like the United States and the United Kingdom, cyberstalking provisions essentially carries 'no contact order' as a civil remedy to restrict the stalker from contacting the victim for a considerable period (Halder, 2015, p.120) Indian laws on Cyber Stalking (both in S.354D IPC and S.11 (iv) and S.12 of the POCSO Act) do not mention anything about such 'no contact order'. The Courts in India have not got much scope to test the effectiveness of this law yet. It is expected that if the courts take up more cautious views to protect the interest of the victims as per the opinion of these authors, the objective of the law may be fulfilled.[31]

Till March 2015, the government used Section 66A of the Information Technology Act as the remedy for all online abuse, but the Supreme Court struck it down as unconstitutional. However, there are provisions under the Indian Penal Code which provide a direct legal remedy to harassment. Despite legal provisions, there are loopholes, says Duggal. After the IT Act amendment, barring a few cyber-crimes, almost all are made bailable offenses. So, there is no deterrent. People know they will be eventually bailed. And after being bailed out, people go back and destroy incriminating evidence. And in many cases, the servers used are outside the country and the government can do only so much.[32]

JUDICIAL PRONOUNCEMENT

In the Digital era, criminals are using a new way of techniques with the help of Information and communication technology to commit a crime. In India, Judiciary has been playing a vital role in combating a new emerging form of cyber-crime. It's the most important and independent wing of the Indian constitution. For the betterment and development of society need specific laws and strong adjudicative authority. As per the Constitution of India, Judiciary is an independent machinery. It has always played a very effective role in each area of law. But looking at Cyber-crime nature, Judiciary should have the technical knowledge to understand the nature of crime and whether it is crime or not. The Indian conventional law like Indian Penal Code 1860 and The Criminal Procedure Code 1973 have had provisions for territorial jurisdiction but these provisions are not sufficient to deal with cybercrimes very effectively. So need specific provisions to deal with exclusively cyber-crime. In Cyber laws there is certain clarification required in cyber-crime and jurisdiction. Reformation should be required in India's conventional laws so the Indian Judiciary could be able to access its powers to curbing cyber-crime in cyberspace. **Chandra Prakash Kewal Chand Jain V. State of Maharashtra**[33], the Supreme Court in this case said that "When the respect of womanhood in our country is, on the decline, unfortunately. In our country, the standard of decency and morality in public life is now the same as in other countries of the world, so decency and morality in public life can be promoted and protected if only the courts deal strictly with those who violate the societal norms". In the digital era, women have been viewed and portrayed as sex objects. But in so many cases Indian Judiciary has been trying to protect women in cyberspace also. Women and young minor girls are softly targeted in cyberspace. In most cases, police have not been able to either collect electronic evidence or preserve it or produce it or prove it. Even if you get a cyber-crime registered, the police invariably do not register these cases because they are not sure if they will be able to crack it. The police are more comfortable with the traditional laws relating to crimes that happen physically. There is no capacity building among law enforcement agencies. So, the majority of these cases had resulted in acquittal, says Duggal. Cyber Law and Information Technology, by Talwant Singh, Additional District and Session's Judge, Delhi, has published his article in Delhi courts.nic.in, a

[30] Available at https://www.aiirjournal.com/uploads/Articles/2016/01/307_04.Dr.Menon%20H.V..pdf (Accessed on 14th December 2020 at 04:09 pm).
[31] Debrati Halder & K. Jaishankar (2017), Cyber Crimes against Women in India, Sage Pub. India Pvt Ltd ISBN: 978-93-859-8577-5 (HB) page no.102.
[32] Available at http://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html (Accessed on 4th November 2020 at 11:30 pm).
[33] AIR 1990 SC 658.

survey indicates that for every 500 cyber-crime incidents that take place, only 50 are reported to the police and out of that, only one is registered.[34] There are so many Cyberstalking cases that have been reported and registered, in one case of Tamil Nadu, A 21-year-old woman from Salem district also a victim of Cyber Stalking. Accused has morphed her pictures and put them on Facebook and tagged her on the post. They have been reported to the cyber cell. After reporting cyber cell she got another morphed image. One more Bangalore's Cyber Stalking Case, in this case, the girl committed suicide. According to the Times of India, on October 5, 2020, 23% rise in cybercrimes against women in Gujarat. The report mentioned that the state police recorded 28 cases of online stalking or bullying, 21 cases of cyber pornography, six cases of blackmail, five cases of fake profiles, and four cases of defamation or morphing – in all the cases, the women were the victims. Overall, the state recorded an 11.7% rise in cybercrimes compared to 2018.[35].There are so many cases of Cyber Stalking against women in India. Specific Cyberstalking against women in India related instances are following:

- **Ritu Kohli Case**: The gravity of cyberstalking came into focus in India with Ritu Kohli's Case, which is the first case in India dealing with cyberstalking. The Delhi Police arrested Manish Kathuria the culprit of the case. In the said case, Manish was stalking a person called Ritu Kohli on the Net by illegally chatting on the website www.mirc.com with the name of Ritu Kohli. Manish was regularly chatting under the identity of Ritu Kohli on the said Website, using obscene and obnoxious language, was distributing her residence telephone number and inviting chatter to chat with her on the telephone. Consequently, Ritu Kohli was getting obscene calls from different chatters from various parts of India and abroad. Ritu Kohli reported the matter to the police and the Delhi Police swung into action. The police had registered the case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli. But Section 509 of the Indian Penal Code only refers to a word, gesture, or act intended to insult modest of a woman. But when the same things are done on the internet, then there is no mention of it in the said section. None of the conditions mentioned in the section cover cyberstalking. Ritu Kohli's case was an alarm to the Government, to make laws regarding the aforesaid crime and regarding the protection of victims under the same. As a result Section 66A of the Information Technology Act, 2008. However critics felt that section 66A would be used as a tool to curb individual freedom of speech and expression and violate Article 19(1) of the constitution of India and in the year 2015 in the writ petition titled Shreya Singhal v. Union of India the Apex court struck down the section 66A of Information Technology Amendment Act 2008, as it is grossly misused by the authorities and violate of Article 19(1) of Constitution of India.[36]
- **Kalandi Charan Lenka vs. State of Orissa (2017):** The informant is a student studying at the Women's College Pattamundai in Pattamundai. Among other items, it is alleged that her father has three daughters and that his first daughter is a mentally retarded girl and that the second daughter is the informant. The victim girl came in her mobile alleging her character while researching unknown obscene messages at School. Before this also from an unknown mobile number, pornographic messages influencing the informant's character also came across her father's cell phone. Her father after passing the message became sorry and told the informant-victim about the matter. Thus the victim's wife became mentally disturbed to see these disgusting texts. The written letters containing obscene language imputing the victim girl's character then came to her father during the year 2015-2016. Those letters came with sexual comments and a template that denigrated the victim girl's character. The messages not only influenced the victim girl's character but also linked the other male members to the victim girl for having sex. The Cyber Cell of the Crime Branch had investigated the same issue, and the High Court held that the accused was prima facie liable for sexual harassment offenses under Section 354A, 354D for cyberstalking under the Indian Penal Code, 1860, Section 66-C for identity theft, Section 66-D for impersonation and Section 67 and 67 for electronic transmission of obscene and sexually explicit content. Therefore the bail application was also rejected.[37]
- **Yogesh Prabhu's Case (2015)**: In July 2015, the Metropolitan Magistrate court convicted a senior executive of a private company in a cyberstalking case for four months imprisonment. This case became the first conviction case of cyber-crime in the state of Maharashtra. Additional Metropolitan Magistrate N. R. Natu convicted and sentenced Yogesh Prabhu to four months imprisonment for cyberstalking to his colleague working in a cargo, handling firm in Panvel.[38]
- **Karan Girotra vs. State & another:** This case reaches the judiciary on cyberstalking. Case deal with the woman, Shivani Saxena, her marriage was not perfectly consummated and filed for a divorce by mutual consent accordingly to the Hindu marriage act, 1955. After that, she came across Karan Girotra through online chatting and propose her marriage. On the pretext of introducing her to his family, Girotra invited Saxena to his house, and tried to give the drug to her, and was sexually assaulted and which was successfully done by him. Girotra

[34] Available at http://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html (Accessed on 4th November 2020 at 11:41 pm).
[35] Available at https://timesofindia.indiatimes.com/city/ahmedabad/23-rise-in-cybercrimes-against-women-in-gujarat/articleshow/78482025.cms (Accessed on 24th December 2020 at 06:58 am).
[36] Available at https://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf (Accessed on 7th October 2020 at 10:09 pm).
[37] Available at https://www.soolegal.com/roar/introduction-of-stalking-into-indian-legal-regime (Accessed on 6th October 2020 at 10:06 pm).
[38] Available at https://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf (Accessed on 6th October 2020 at 10:29 pm).

had started sending her obscene pictures. He had started extorting her to circulate obscene pictures if she refuses to marry him. Shivani Saxena had complained about Section 66-A IT Act on the ground of obscene and nude pictures of Shivani Saxena which was circulated by Karan Girotra. This act requires a serious custodial interrogation. The court observed that there is an occurrence of filing FIR by Shivani Saxena and she had consented to sexual intercourse and also decided to file a complaint against Girotra as he had refused to marry her. This leading case highlights the mark of the Indian judiciary regarding the case of cyberstalking or bullying.[39]

❖ **President Pranab Mukherjee's Daughter's Stalking Case:**

Sharmistha Mukherjee, daughter of President Pranab Mukherjee, was allegedly harassed by a man, who posted sexually explicit messages on her Facebook page. She complained to the Cyber Crime Unit of Delhi Police. Police said the "lewd" messages were sent to the complainant through Facebook Messenger. The profile of the sender mentions him as a resident of Naihati in Hooghly, West Bengal. Mukherjee shared screenshots of the messages sent to her and said she decided to speak up against online harassment as ignoring it would only encourage him further. She also tagged the man who has now deleted his profile from Facebook.[40]

SUGGESTIONS

There are following suggestions which give protection to individual from victimization of cyberstalking and would able to curb cyberstalking offense:

- In Information Technology Act 2000 need amendment and required specific provisions which solely deal with Cyber Stalking. Apart from that uniformity in legislation to define Stalking, amendment in criminal law, and continuous training to enforcement agencies should be required for combating cyber-crime.
- Coordination and Cooperation between Internet Services Provider and all enforcement agencies should be required to combat the increasing Cyber-crime.
- One should have to be aware of fraudulent websites which used to steal personal information.
- One should have to take cognizance of the privacy policies of websites and software.
- One should have to avoid phishing emails, setting a password and change it regularly and also set safety measures, not share personal information on social media and avoid chatting with strangers and install the latest version of Antivirus software on all devices.
- One should have informed the local police or cyber cell in case of Cyber Stalking.
- To combating Cyber-crime against women that self-awareness regarding cyber-crime and self-regulations are the best methods.
- Government has to take efforts to bring cybercrimes awareness and its legal remedies available in Cyber Law and Indian Penal Code 1860 with allied laws in society.

CONCLUSION

In India, there is no specific legal provision which directly gives protection to cyber stalking's victim. Some provisions of the Information Technology Act 2000 and the Indian Penal Code 1860 give indirect protection against cyberstalking. While other countries have specific legislation on Cyber Stalking. So this is the main lacuna in Indian Legislation. Apart from that, legal officers and law enforcement machinery need continuous training regarding a new form of cyber-crimes. Cyberstalking has geographical limitations to the concerned country. So international machinery has to think to make specific global legislation for cyberstalking. The Indian Judiciary has been very conscious, sensitive and acted as the ardent and protector of individual rights. In this paper, the brief of the above-mentioned judgment shows that the Indian Judiciary has played a vital role to protect women from various types of exploitation in cyberspace.

[39] Available at https://www.researchtrend.net/ijet/pdf/Cyber%20Stalking%20Technological%20Form%20of%20Sexual%20Harassment%20Shivam%20Jindal.pdf (Accessed on 11th December 2020 at 04:45 pm).

[40] Available at http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html (Accessed on 20th October 2020 at 12:02 pm).