International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Crimes of Stalking and Harassment Against Women in Cyberspace

Amit Kumar[1], Dr. Dalip Kumar[2]

[1]Assistant Professor, Army Institute of Law, Mohali
[2]Professor, Department of Law, Kurukshetra University

Abstract

With the advancement of technology the world has become a global village. The most modern invention is the Internet which has broken national boundaries and has created a space known as cyberspace. The Internet is the new oil of the 21st century. Like any invention, the internet too has both boon and bane. Crimes against women are rising against women in every sphere of life. Crimes against women start with her fetus in the form of female feticide, when she is born in the form of female infanticide, in her youth matrimonial crimes, sexual crime and so on. With the coming of the internet and a new space have emerged which have become the playground for offences against women. Cybercrime is the most burning issue in contemporary times affecting the modesty; security and privacy of net users especially women. This paper is an attempt to highlight the legal provisions dealing with cyber stalking and harassment against women in India.

Keyword: Cyber Crimes, Stalking, Harassment, IT Act, Sexual Harassment, Internet

Meaning of Cyber Crimes

The Indian legislature has failed to specify the definition of *"cyber crime"* in the Information Technology Act, 2000 or any other law. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime."[1]The Oxford Dictionary defined the term cyber crime as "Criminal activities carried out by means of computers or the Internet."[2] Dr. Debarati Halder and Dr. K. Jaishankar define cyber crimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".[3] Professor S.T. Viswanathan has given three definitions in his book *The Indian Cyber Laws with Cyber Glossary* is as follows, "any illegal action in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer; any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have

[1] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 16th March, 2023)
[2] http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 17th April, 2023)
[3] http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf (Accessed on 17th October, 2023)

made a gain; computer abuse is considered as any illegal, unethical or unauthorised behaviour relating to the automatic processing and transmission of data."[4]

Cyber Stalking

Cyber Stalking is a unique form of cybercrime. The advent of the internet has made it possible to converse with others through email or other social media platforms such as whatsapp, facebook, instagram, twitter etc. Cyber-stalking is an example of how humans can even misuse the good things in the worst possible manner.[5] It is a serious offence which leads to the violation of anti-stalking laws, slander laws and harassment laws. It is majorly observed that the majority of online stalkers are males and the victims are females. It has been researched that there is a prior relationship between cyber stalkers and victims. However it is not uncommon that cyber stalking is performed by strangers.[6]

The bane of the technology is such that a cyber-stalker can get the victim's personal information via a few keystrokes on the computer through a social media platform. Through social media platforms, a stalker can easily access personal information and get quick access to personal information and take undue advantage. Cyber stalkers also sometimes resort to threats of publishing their personal information against their consent.[7] "Cyber stalking is also called cyber teasing. Anyone who via email or certain messages in electronic form tries to accuse a person or defames his prestige in the society is said to be cyber-stalker." There are two different types of cyber stalking which are :

1. Harassment and cyber stalking start and continue online.
2. When such a potential stalker attempts to trace the victim's telephone number or home address, such an action leads to online harassment and offline harassment.

Cyber-stalking takes many forms, however its characters are akin to offline stalking. Both are intended to extend control over their victim. However online cyberstalking is more dangerous as there are no territorial limits.[8]

Cyber Stalkers

A cyberstalker is a person connecting to a person known or unknown to them without their permission or wishes through the internet.[9] The cyberstalker may be categorised as simple obsession stalkers, love obsession stalker, erotomanic stalkers, delusional cyber stalkers, vengeful cyber stalker, organised stalker, false victimisation syndrome stalker, incompetent stalkers, predatory stalkers, intimacy seeker stalkers, resentful stalker, celebrity stalkers, political stalkers etc. The motivation for the cyber stalker include obsessiveness, delusion, obsession for love, sexual desire, ego, mental illness, rejection , anger.

[4] Viswanathan, Suresh T, Indian Cyber laws with Cyber Glossary, Bharat Law House New Delhi, 2001 p.81.
[5] Pittaro M. Cyber Stalking : An Analysis of Online Harassment and Intimidation, International Journal of Cyber Criminology, Volume I(2) (2007)
[6] Verma A. Cyber Crimes in India, Central Law Publications, Allahabad, 2017 p. 131
[7] Rao S., Cyber Stalking (A Real problem, the virtual world), The lawyer collective p. 21
[8] Rathor and Das, "Cyber Crime: The Emerging trends and challenges", CyberSpace and Law : Issues and Challenges, NALSAR University, Hyderabad, 2004 p. 102
[9] Snook A., "Stalking in the workplace the complete guide to prevention and investigation", available at: https://www.i-sight.com/resources/stalking-in-the-workplace-the-complete-guide-to-prevention-and-investigation

Harassment and Cyberstalking

Cyber Stalking and Harassment are almost correlated concepts that involve one or more people terrorizing and menacing another person. Stalking relates to following people, while harassment includes behaviours designed to create nuisances. Harassment also involves willful acts of repeated harassment to threat, intimidation, harassment or teasing which causes an ordinary person to be annoyed. Both Cyber Stalking and Harassment are transnational crimes. Offences may get committed in one country and consequences may fall in another country. They pose a challenge to the conventional jurisdictional realms of the sovereign nation. Sometimes, they become infeasible to investigate and prosecute such crimes due to inaccessible jurisdiction.

Anonymity is another peculiar feature of these offences. In most cases, the victim does not know who the stalker is. On the internet the predator can hide their identity and possess a hindrance in the prosecution of the offences. It has also been observed that stalkers use sophisticated technology to further hide their identity and sometimes they even create fake I.P. Address to enhance anonymity. The cheaper internet connection with minimum effort and a large amount of information can be transmitted to multiple destinations which poses a major threat to the victims.

Typology of Cyber Stalking and Harassment

Smart phones today have somewhat replaced the old computer and now the connection to cyberspace is in the palm of the individual. The primary ways in which cyber stalking is done are email stalking, social networking sites stalking, computer staking where the offender takes control of the operating system of the victim, chat stalking and stalking through the Bulletin Board system. Apart from these there are other kinds of stalking that exist. They include spouse stalking, family member stalking, corporate stalking, workplace violence staking.

Online harassment is most prevalent these days and women are the biggest victim of the crime. The online harassment includes in the form of online impersonation, catfishing, doxxing, swatting, trolling, revenge porn, cyber bullying, hateful speech, online threats, cyber mob attacks etc. The factors responsible for online harassment are disproportionate presence of men online, anonymity, dimensional communication and jurisdictional issues.

National Legislation

The term stalking as an offence is provided in Indian Penal Code, 1860 under section 354D[10]. The section was inserted by way of amendment in 2013. Justice Verma Committee[11] was setup to

[10] Section 354 D IPC, 1860 provides

(1) Any man who—

1. 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
2. monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking[1];

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

1. 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
2. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
3. 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.

recommend changes in the law and bring more inclusiveness of sexual crimes. In the recommendation the Indian Penal Code, 1860 was amended and new offences relating to making sexually harassment[12] and sexual voyeurism[13] were included.

The offence of *'Obscenity'* is also provided under the IPC under section 292. The act of cyber stalking takes within its purview the act of sending obscene material to the victim on a social networking site or through email or messages etc. where the stalker harasses the victim by sending obscene material through the internet and he can be held guilty under the aforesaid section. Similarly offences of *'Criminal Intimidation'*[14], *'Intentional Insult with intent to provoke breach of peace'*[15] and '*Words, gesture or act intended to insult the modesty of a women'*[16] are also provided and can be used against the stalkers. Section 499 of the IPC Act, 1860 further provides punishment for *defamation* and in cyber crimes offence of defamation comes under the purview of online harassment. Section 499 explains defamation as *"Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person."*

The provisions of Information Technology Act, 2000 does not deal with the incidents of trolling directly. Section 66A of the IT Act, 2000 deals with the Punishment for sending offensive messages through communication service etc. According to this section whoever sends any offensive or annoying message through a computer resource or communication device will be sentenced for a period that may

[11] Accessed on https://prsindia.org/policy/report-summaries/justice-verma-committee-report-summary
On December 23, 2012 a three member Committee headed by Justice J.S. Verma, former Chief Justice of the Supreme Court, was constituted to recommend amendments to the Criminal Law so as to provide for quicker trial and enhanced punishment for criminals accused of committing sexual assault against women. The other members on the Committee were Justice Leila Seth, former judge of the High Court and Gopal Subramanium, former Solicitor General of India.

[12] Section 354A Indian Penal Code 1860. *Sexual harassment and punishment for Sexual Harassment*
(1) A man committing any of the following acts-
(i) physical contact and advances involving unwelcome and explicit sexual overtures; or
(ii) a demand or request for sexual favours; or
(iii) showing pornography against the will of a woman; or
(iv) making sexually coloured remarks, shall be guilty of the offence of sexual harassment.
(2) Any man who commits the offence specified in clause (i) or clause (ii) or clause (iii) of sub-section (1) shall be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both.

[13] Section 354-C. Indian Penal Code, 1860 *Voyeurism*.- 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 on first conviction with imprisonment of either description for a term which shall not be less than one year, but 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 shall not be less than three years, but which may extend to seven years, and shall also be liable to fine

[14] Section 503. Indian Penal Code,1860 *Criminal Intimidation.* —Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intim-idation.

[15] Section 504. Indian Penal Code,1860 *Intentional insult with intent to provoke breach of the peace.*—Whoever intentionally insults, and thereby gives provoca-tion to any person, intending or knowing it to be likely that such provocation will cause him to break the public peace, or to commit any other offence, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

[16] Section 509. Indian Penal Code,1860 *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 with simple imprisonment for a term which may extend to one year, or with fine, or with both

extend to three years and with fine.[17] It is non bailable and cognizable offence. This section of the IT Act, 2000 was inserted to curtail the incidents of stalking, phishing and spamming. The terms "annoyance and inconvenience" used in the section do not have a clear meaning in criminal law. If a person i.e. a troll writes something which does not offend or hurt the sentiments another person or the police officer feels that it does not offend or hurt, then this section will not apply. Section 67 of the IT Act, 2000[18] is a copy of section 292 of the IPC, 1860. This section deals with the publication of obscene material in electronic form. If a stalker attempts to disseminate any obscene material about the victim, he will be charged under section 67. Section 67A IT Act, 2000[19] inserted after 2008 amendment provided penalty for publishing or transmitting content containing sexually explicit material. Section 67 B[20] also inserted by the 2008 amendment provided punishment for publishing or transmitting material depicting children in sexually explicit acts etc. in electronic form and cyber stalking.

Section 67C IT Act,2000[21] provides punishment for identity theft relating to cyber stalking as cyber stalkers often use somebody else's identity. For example they create an email account in another individual's name to never know their real identity. Thus, they commit identity theft, a cyber offence in itself is to commit another cyber offence, namely cyber stalking.

[17] *Shreya Singhal v. Union of India* (2013) 12 S.C.C. 73. The Supreme Court struck down Section 66A of the Information Technology Act, 2000, relating to restrictions on online speech, as unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the Constitution of India. The Court further held that the Section was not saved by virtue of being a 'reasonable restriction' on the freedom of speech under Article 19(2).

[18] Section 67 Information Technology Act, 2000 *Punishment for publishing or transmitting obscene material in electronic form.* -Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

[19] Section 67A Information Technology Act, 2000 *Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form*. -Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

[20] Section 67B Information Technology Act, 2000 *Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.* -

Whoever- (a) publishes or transmites or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually esplicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

[21] Section 66C Information Technology Act, 2000 *Punishment for identity theft.* -Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

Judicial Response

Both the National as well as International judiciary has come to the rescue of the victim and punishing the perpetrators of the crimes. The proactive approach of the judiciary can be visible through various pronouncements. In *Manish Kathuria Vs Ritu Kohli,*[22] the gravity of the offence of cyber stalking came into focus in India. When Delhi based Ms. Ritu Kataria filed a complaint against Manish Karthuria to Delhi Police, who was using her identity to chat over the internet. The same person was also deliberately giving her phone number to other chatters encouraging them to call Ritu at odd hours. This case was warning bells for the government of India. The judiciary analysed that Ritu Kohli's case can be registered under only section 509 IPC.As a result, section 66A of the IT Act, 2008 was enacted to punish cyber stalkers and section 354D was added in 2013 to define stalking as crime. This became the reason for the 2008 amendment to the IT Act.

In *State(Cyber Cell) v. Yogesh Pandurang Prabhu,*[23] is one of the first cases of conviction under section 354D IPC read with section 66A & 67 of the IT Act,2000. According to the facts of the case one Yogesh Prabhu stalked his own colleague and used to send her pornographic images and videos through fake email id and name. In *Avinash Bajaj v State*[24] the court held, "whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished." In *Nipun Saxena v. Union of India,*[25] Supreme Court held, "section 228-A imposes a clear bar on the name and identity of the victim being disclosed. Therefore, where the accused is acquitted and the victim of the offence wants to file an appeal under section 372 Cr.P.C., she is not bound to disclose her name in the memo of appeal. Such a victim can move an application to the court praying that she may be permitted to file a petition under the pseudonymous name e.g. "X" or "Y" or any other such coded identity that she may choose. Any document disclosing the name and identity of the victim should not be in the public domain."[26]

In *Tamiz v. Google Inc.*,[27] the Appellate Court held that, "Google is an online platform, which is vicariously liable for publishing a defamatory material, as "publisher" if it does not act immediately

[22] C.C. No. 14616/2014

[23] CC No. 3700686/PS/2009 Chief Metropolitan Magistrate, Mumbai. The trial court convicted the accused of one month simple imprisonment with a fine of 1000 rupees under section 509 IPC. Court further convicted the accused for 3 month simple imprisonment and fine of rupees 10,000 under section 66E IT Act.

[24] 2008 (150) DLT 769. This case involved an IIT Kharagpur student Ravi Raj, who placed on the baazee.com a listing offering an obscene MMS video clip for sale with the username alice-elec. Despite the fact that baazee.com have a filter for posting of objectionable content, the listing nevertheless took place with the description, "Item 27877408 – DPS Girls having fun!!! full video + Baazee points." The item was listed online around 8.30 pm in the evening of November 27th 2004 and was deactivated, around 10 am on 29th November 2004. The Crime Branch of Delhi police took cognizance of the matter and registered an FIR. Upon investigation, a charge sheet was filed showing Ravi Raj, Avnish Bajaj, the owner of the website and Sharat Digumarti, the person responsible for handling the content, as accused. Since, Ravi Raj absconded; the petition was filed by Avnish Bajaj, seeking the quashing of the criminal proceedings.

[25] (2019)2 SCC 703.

[26] Ibid. *para 28 & 50.4*

[27] [2013] EWCA Civ 68. In this case a claim was brought against Google Inc and Google UK Ltd. According to facts comments were posted on the blog named 'London Muslim' blog. The Blog was hosted on Blogger.com which was operated by Google Inc. The plaintiff had complained to The Google had contacted the author of the Blog after some delay who then voluntarily removed it. The claim was in relation to the comments, which were published on "The Blog" during the period after Google Inc. had notified the comments but before their removal.

upon such notification or complaint."[28] In *Zeran v. America Online Inc.*,[29] the U.S Court held that, "AOL was not liable for a false advertisement placed on an AOL bulletin board, which directed the users to call plaintiff and which resulted in him facing significant harassment." In *United States v. Sayer*,[30] the landmark judgement came in which the accused was convicted for cyber stalking and revenge porn and court sentenced him for 5 year imprisonment.

Conclusion and Suggestion

As the cyber world is expanding, with the advancement of technology the offense of cyberspace has entered by household and hands. Cyber stalking and cyber harassment crimes are rapidly increasing. Though there exists legislation like penal provision in IPC and IT Act 2000. However effective cyber stalking regulation is still required. Many offenders skip punishment due to lack, of effective legislation and implementation. There is a need to educate the law enforcement agency on the process of collecting evidence. Development and procurement of the enforcing and detection infrastructure is also needed. It is to be kept in mind that cyber stalking crimes also escalate in more heinous crimes such as murder, rape, abetment of suicide and other forms of assault. Women who are the most prone victim of the crime also need to take safeguards such setting up of separate email account for personal and professional needs, changing the privacy setting if the social media account, regular changing of passwords, avoiding connecting to the public internet connection etc.

[28] Ibid.

[29] 129 F.3d 327 (4 Cir. 1997) In this case, the plaintiff named Karneth Zeran became a victim of trolling. Soon after the Oklahoma City bombing, the plaintiff was defamed by an unknown America Online (AOL) subscriber by posting an advertisement that Mr. Zeran was selling t-shirts regarding the bombing of the Alfred P. Murrah Building fee Oklahoma City. The unknown subscriber also mentioned the plaintiff's house telephone number and home address from where he carried his business. Due to all this he was subsequently being harassed. He was inundated with complaints and death threats also.

[30] 748 F. 3d 425 (1st Circuit. 2014) According to the facts of the case the accused Sayer used to stalk his ex-girlfriend and started posting her address and morphed photographs. He encouraged people to show up at her hose asking for sexual favours.