CYBER CRIME AGAINST WOMEN: ISSUE OF VIOLATION OF RIGHT TO PRIVACY AND RIGHT OF DIGNITY

Ms. Asmita B. Kavathekar (Research Scholar at ILS Law College, Pune)

Abstract

While crime against women is on the rise in all areas, being a victim of cybercrime can be the most traumatic experience for a woman. Especially in India, where the society looks down on women and the law does not even recognize Cyber Crimes against them properly. In this paper, I will discuss various kinds ofCyber Crimes that can be committed against women and how they violate her right to privacy and right to dignity. I will also briefly discuss the various laws that are existing in India to protect women in such cases, such as the Information Technology Act (2000) and other Constitutional provisions. I also take an in-depth look at the recent rise in online crime against women and its various causes. The right to privacy has been freely interpreted by Hon'ble Supreme Court under Article 21 of the Constitution of India. I will suggest several measures to combat the ever-increasing cybercrimes against women in India. In short, Iam focusing on the remedies available to victims of cybercrime and the necessary changes in the legal system to effectively curb the growth of cybercriminals.

- **INTRODUCTION**

The safety of women has been an issue especially in a country like India where traditional crime rates against women are increasing rapidly. Nowadays, cybercrime against women is a very well-known issue. Every second woman in India is a victim of cyber crimes and online podiums are now a new platform where a woman's privacy, dignity and her safety is being questioned more and more at every moment. Technology is a means used by some criminals who try to defame women by sending obscene emails, WhatsApp messages, stalking women through websites, using chat rooms, and worst of all, developing pornographic videos, mostly created without their consent, and fraud convert letters, images into pornographic content through various programs available online. Indian women are not very much comfortable to immediately report the cybercrimes to Police stations because they don't really know where to report such crimes or they don't take reporting seriously because of the social embarrassment that they don't want to face while living in society. In cybercrimes against women, the impact is mental rather than physical, while the focus of laws to ensure the safety of women is physical rather than mental harm. At this point, it can be said that especially women's world of thought must be broadened and they must be a whip to restrain criminals, i.e. file a complaint immediately against cyber criminals. Most problems will be solved if women immediately report the crime and warn the abuser about taking strict legal action against him.

- **MEANING OF CYBER CRIME**

Cyber Crime is the crime which involves computer and a network / internet for commission of crimes. With the advent to technology, Cyber Crime and victimization of women are increasing. In its broader sense, cybercrime refers to any illegal behaviour that uses or relates to a computer system or network, including crimes such as the illegal possession, transmission or sharing of information using a computer system. Cybercrime originates or starts from trying to break into computer networks by hackers. Some did it simply for the thrill of accessing high level security networks or tapping into sophisticated security networks, but others sought to obtain sensitive or classified material. Eventually, criminals began to infect computer systems with computer viruses, which led to the destruction of personal and business computers. With the advent of computers in the late 1960s, crimes were mostly related to damaging computer networks and physical telephone networks.

Computer viruses are forms of code or malware programs that can copy themselves and damage or destroy data and systems. If computer viruses are widely used, such as in banking, government or hospital

networks, these activities can be classified as cyber terrorism. Computer hackers also engage in phishing scams, such as asking for bank accounts details and credit card theft. Hacking is a term used to describe the act of modifying a product or procedure to change its normal operation or solve or fix the problem. The term originated in the 1960s when it was used to describe the activities of certain model train enthusiasts at MIT who modified the operation of their model trains. They found ways to change some features without redesigning the entire device. The harmful association with hacking emerged in the 1970s when early computerized telephone systems were targeted. This innovative type of crime was a difficult problem for law enforcement, partly due to the lack of legislation supporting criminal prosecution and the lack of crimes. researchers familiar with hacking technology. It was clear that the computer systems were open criminal activity, and as more complex communications became available to the consumer, more opportunities for cyber crime developed.

- **REASONS FOR GROWTH IN CYBER CRIME CASES AGAINST WOMEN IN INDIA**

As this is very much clear that statute deals with cyber crime is not expressly mentioning those crimes under the related sections whereas on the other hand various laws such as IPC, Constitution give special protection to women, but the same protection seems not to be given in general under the specific statute. But in most cyber crimes, there were additional reasons that contributed to their not being reported, such as the victim's reluctance and shyness or her fear of a defamation against family name. As this is very much clear that statute deals with cyber crime is not expressly mentioning those crimes under the related sections whereas on the other hand various laws such as IPC, Constitution give special protection to women, but the same protection seems not to be given in general under the specific statute. But in most cyber crimes, there were additional reasons that contributed to their not being reported, such as the victim's reluctance and shyness or her fear of a defamation against family name.

- **LEGAL REASONS**

The purpose of the IT Act is crystal clear from its preamble, which states that it was mainly created to improve electronic commerce, so it covers commercial or financial crimes such as hacking, fraud, breaches of confidentiality, etc., but the drafters were not aware. of the protection of online users. As we discussed above, most cybercrimes are prosecuted under sections 66 (hacking), 67 (publication or transmission of obscene material in electronic form) and 72 (breach of confidentiality). These provisions deal with the majority of online crimes that are not related to online shopping. Cyber defamation, internet defamation, email fraud, cyber sex, hacking and invasion of privacy are very common these days, but the IT Act does not mention them in any sections or provisions. While the IPC, Criminal Procedure Code and the Constitution of India offer special protection to women and children, for example, women's modesty is protected under Section 509 and rape, forced marriage, kidnapping and abortion against a woman's will are crimes and prosecuted under the IPC. The Indian constitution guarantees women equal rights to housing, education, health, food and work, but until recently there were no specific penal provisions to protect women from cybercrimes. Ever since the Delhi gang rape in 2012 (Nirbhaya case), there has been a huge outcry for new reforms in the criminal laws to protect women from criminals. The Penal Code Amendment Ordinance 2013 contains several additions to the Indian Penal Code such as Sections 354, 354 A, 354 B, 354 C and 354 D, through these sections, now MMS scandals, pornography, morphing, defamation can properly treated. As mentioned earlier that crossing the Internet is one of the main reasons for the growth of cybercrime, Section 75 of the IT Act deals with crimes or offenses committed outside India but does not talk about the jurisdiction of the offences committedin cyberspace.The issue of place of reporting arises especially when a crime is committed in one place, affected person that is victim is in another place and then reported in another place. Although in most cases the Code of Criminal Procedure is followed according to territorial jurisdiction'

- **SOCIOLOGICAL REASONS**

Most cybercrimes remain unreported due to the hesitation and shyness of the victim and fear of defamation of the family name. She often thinks that she herself is responsible for the crime committed against her. The women are more vulnerable to the threat of cybercrime because the perpetrator remains anonymous and can constantly threaten and blackmail the victim using different names and identities. Women fear that reporting the crime may make their family life difficult. They also doubt about getting help of their family in such cases and what impression society has of if society could know about the cyber crime is committed against her. Because of these fears, women often do not report crimes, which further encourage the perpetrators to commit the crimes.

Cybercriminals use computer technology to access personal information and use the Internet for harassment and exploitation, including stalking, blackmail and threats through the emails, photo editing that is morphing, cyber pornography etc. Nowadays, criminals are gradually misusing cyber platforms to harass and exploit women in India for curious pleasures. Women mostly suffer from cyber stalking, harassment, extortion, blackmail etc. Women often trust criminals or abusers or due to lack of knowledge of privacy and account settings of phones and social media accounts, they often share their personal information, leading to many cyber crimes. Often, criminals get the opportunity to harass, abuse, blackmail, etc. Women and children in this form of cases, are abused more because they do not know the complaint procedure. Cybercrimes against women, usually through fake IDs created on Facebook, Twitter and other social media, cause serious harm to women and their privacy and dignity as criminals use these platforms to carry out extensive blackmail, threats, harassment or deception through instant messages and emails. Men with bad intentions commit these cybercrimes with malicious intentions such as illegal gain, revenge, insulting women's modesty, blackmail, extortion, sexual abuse, defamation, inciting enmity against a community, mocking to gain control and stealing information.

- **Forms Of Online Crimes Against Women**

Amongst the various cyber-crimes committed against individuals and society at large, crimes that are targeting women are as follows:

- **Cyber Stalking**

One of the most common Cyber Crime nowadays against women is Cyber stalking which includes following someone silently or tracking someone's activities in an online or offline mode for gathering knowledge or personal information of other person without their consent. Stalking means intrusion in person's privacy in order to terrorizes, harass, torture or to intimidate the victim. The offender tries to contact the victim and forms a relationship without his or her consent.

It will include cyber crime when such actions are done purposefully through internet, email or by any other electronic form of communication which includes cracking or hacking any password for the same purpose or someone uses identity of the woman for the same. In many incidents, devices of victims are hacked in order to obtain private content on any electronic device which is later used to blackmail them or to keep a check on them. In some case, mobile phones are hacked to destroy the evidence against the offender.

- **Cyber pornography**

It is a conduct of creating, publishing, communicating pornographic materials by using the cyber space. Circulating images / video clips of women engaged in intimate acts As we know certain acts of prurient conduct which are especially pointed to intimate acts of women are increased in the modern times under IT Act, which provides for pictures and videos to be easily captured on a single click and can be communicated as widely as one can reach through porns and social networking sites via internet.

- **Morphing** This includes improvising or editing the real picture by a fake or an unauthorized user by the way of creating fake profile and then downloading the victim's photograph from internet and then edits

it in a manner which harms the original identity of the victims and posts it on the social networking sites or by any mode which can harm the reputation of the victim. It is now so common process that anyone can use such process for taking revenge or for fun purpose which dangers the modesty of the woman.

It includes attaching the photograph of the victim to a photograph which have nudity or skimpy clothes of another woman by the use of such automated software which are available easily and can malign the image or the character of the victim easily in front of a larger public. Celebrities are the most common target of all the time for the sake of fun.

- **Sending Obscene / Defamatory / Annoying Messages**

Under this head, acts included are such as circulating private pictures of a woman, posting her pictures with contact details on websites with obscene content amounts to cyber-crime against women. This also amounts to defamation as it affects the privacy of the women which is a fundamental right. Sending of obscene, annoying messages can be through WhatsApp, mail or any other social media platform.

- **Online trolling / bullying / blackmailing / threat or intimidation**

The list of cyber-crime against women includes online trolling/bullying/ blackmailing/ threat or intimidation. This is most prevalent in recent times. Bullying means a repetitive behavior of a person against another with an intention to harm the reputation or demean the same with superior strength or dominant position. It is done by using mobile phones or computer with internet connection. In such situation, internet acts as more like a bane than boon.

- **Legal Provisions Under Various Laws**

Although a comprehensive regulatory framework with regard to laws governing the cyber space, particularly such acts is yet to be framed, there exists certain legal provisions under various Statutes which can come in aid of a person who is a victim of cyber violence.

I. The Indian Penal Code, 1860

Prior to 2013, no law directly dealing with online harassment or crimes pertaining to women in the cyber space was prevailing in Indian Criminal Justice system. In the year 2013, Criminal Amendment Act to the Indian Penal Code, 1860 by way of adding Section 354A to Section 354D, was introduced.

1. **Section 354A**: A man committing any of the following acts – a demand or request for sexual favours; or showing pornography against the will of a woman; or making sexually coloured remarks, shall be guilty of the offence of sexual harassment, may be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both. In case of the first two and with imprisonment of either description for a term which may extend to one year, or with fine, or with both.
2. **Section 354C** defines 'Voyeurism' as including the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her consent. For the act to qualify as 'Voyeurism', the circumstances must be such where the woman would "*usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator*". A person convicted under this section is liable to be punished with fine as well as imprisonment up to three years on first conviction and seven years on subsequent convictions.
3. **Section 354D** introduced a provision for stalking which also covers cyber stalking. Stalking has been defined to mean an act where a man follows or contacts a woman, despite clear indication of disinterest to such contact by the woman, or monitors the cyber activity or use of the Internet or electronic communication of a woman. A man committing the offence of stalking would be liable for imprisonment up to three years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to five years and with fine.

Other than the specific amendments that have been made to the Code, there exist certain other provisions under which cyber crimes may be reported or the accused may be charged. These are:

1. **Section 499**: To defame a person is to do an act with the intention of harming the reputation of the person. Defamation by publication of visible representations of an imputation concerning the woman,

when done with the intention to harm her reputation, is punishable with imprisonment for a term, which may extend to two years, or with fine, or both.

2. **Section 503**: Threats made to any person with injury to her reputation, either in order to cause alarm to her, or to make her change her course of action regarding anything she would otherwise do/not do is punishable as criminal intimidation. The act of blackmailing a person on the internet, as was done in the case mentioned above can be brought within the ambit of this provision.

3. **Section 507**: This provision provides the quantum of punishment for Criminal Intimidation when the same is by a person whose identity is not known to the victim. Any anonymous communication, which amounts to criminal intimidation under Section 503 stated above, is punishable under this section.

4. **Section 509**: Any person who utters any word or makes any sound or gesture, or exhibits any object with the intention that such word, sound or gesture or object be heard or seen by a woman and insult her modesty, or intrudes a privacy, may be charged under this section and imprisoned for a term that may extend to 3 years and also with fine. Instances of lewd comments or remarks made over the Internet, or other explicit images and content forcibly shared over the web may be penalized under this section.

II. The Information Technology Act, 2000 as amended by the Information Technology Act, 2008

When India started journey in the field of information technology, the priority was given to the protection of e-commerce, along with Cyber Crimes, but crimes against women did not find greater emphasis. The Indian legislation has laid down various provisions dealing with Cyber Crime under The Information Technology Act, 2000. The objects enshrined in the Information Technology Act is to provide for legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. In the year 2008, the Information Technology Act has been amended to address issues that the original bill failed to cover and to accommodate further development of Information Technology and related security concerns since the original law was passed. The amendment was made with addition of several provisions.

1. **Section 66C** of the IT Act makes identity theft a punishable offence. Instances of cyber hacking would be covered by this provision. Under this provision, 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 which may extend to rupees one lakh.

2. **Section 66E** of the IT Act deals with the violation of the privacy of a person. Capturing, publishing or transmitting the image of a private area of any person without her consent, under circumstances violating her privacy, is punishable with imprisonment, which may extend to three years, and/or fine.

3. **Section 67** prohibits, and punishes with imprisonment extending up to three years and fine for first conviction and to five years and fine upon second conviction, the publication, transmission and causing of transmission of obscene content. Obscene content has been defined in the same manner as in **Section 292 of IPC**, and therefore the test of obscenity is to be the same as under that provision

4. **Section 67A** makes the publication, transmission or causing of transmission of sexually explicit material punishable with imprisonment extending up to five years and fine for first conviction and to seven years and fine upon second conviction.

5. **Section 67B** makes publication/transmission of sexually explicit content depicting children punishable.

III. Indecent Representation of Women (Prohibition) Bill, 2012

- The Indecent Representation of Women (Prohibition) Act regulates and prohibits the indecent representation of women through the media of advertisements, publications etc. The Indecent Representation of Women (Prohibition) Amendment Bill, 2012 seeks to broaden the scope of the law to cover the audio-visual media and content in electronic form, and distribution of material will also include distribution on the Internet and the portrayal of women over the web.

- **RIGHT TO PRIVACY AND CONSTITUTIONAL LIABILITY**

Crime against women is an act gender-based violence that results in physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether in public or private life. Right of dignity and privacy are the integral parts of fundamental rights of every individual. Every citizen of India enjoys and ensured these rights by virtue of various provisions of Constitution of India and "the right to privacy is protected as an intrinsic part of life and personal liberty under article 21 and as a part of freedoms guaranteed by Part III of the Indian Constitution." However, misuse of advancement in technology violating women's dignity, confidentiality and privacy.

Hacking someone's private property or stealing someone's intellectual work completely violates their right to privacy. The Constitution of India does not expressly provide for the "right to privacy" as one of the fundamental rights guaranteed to citizens of India. The right to privacy is an important natural need of every person because it creates boundaries around a person to which others have limited access. The right to privacy prohibits intrusion into the private lives of others. The Supreme Court of India has clearly established in its legal pronouncements that the right to privacy is largely a part of the fundamental right guaranteed by Article 21 of the Constitution of India. Thus, the right to privacy falls within the purview of Article 21 of the Constitution of India. Therefore, if it is a Cyber Crime involving the private property of individuals or their personal assets, the accused can be charged for violating Article 21 of the Constitution of India and the prescribed measures can be taken against the accused.

- **Infringement of right to Privacy-**

The display of information in cyber world has a close nexus to right to privacy. Right of privacy means, "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the Law against such interference or attacks." Confidentiality refers to information which is told to someone will be kept secret from reach of unauthorized people until the parties agree to uncover the information. Now a days internet has become a vital communication medium and people use their freedom of speech and expression guaranteed under the Indian Constitution. But this freedom is not absolute therefore changes are done in the IT Act also.

In Shreya Singhal vs Union of India, The Supreme Court struck down Section 66 A 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 struck down Section 66A of the IT Act in its entirety holding that it was not saved by Article 19(2) of the Constitution on account of the expressions used in the section, such as "annoying," "grossly offensive," "menacing,", "causing annoyance. Apart from not falling within any of the categories for which speech may be restricted, S66A was struck down on the grounds of vagueness, over-breadth and chilling effect.

- **Right to privacy vs. Social Morality**

Supreme Court of India in the case of Mr. 'X' v. Hospital 'Z' has recognized an individual's right to privacy as a facet Article 21 of the Constitution of India. Itwas alsopertinently held that the right which would advance the publicmoralityor public interest would alone be enforced through the process of court, for thereason that moral considerations cannot be kept at bay and the Judges are notexpected to sit as mute structures of clay in the halls known as the courtroom, buthave to be sensitive, "in the sense that they must keep their fingers firmly upon the pulse of the accepted morality of the day."

Vasunathan v. The Registrar General' has also recognized the "right to be forgotten" and 'Right to be left alone 'as an integral part of individual's existence. Supreme Court held that purpose limitation is integral for executive projects involving at a collection-unless prior permission is provided, third parties cannot be provided access to personal data.

- **Crime against Dignity of Women-**

"The importance and the value that the person has, that makes other people respect them or makes them respect themselves" that means dignity of person. Article 19(1)(a) of the constitution provides fundamental right to speech and expression. This right is not absolute and is subject to reasonable restrictions that are mentioned under Article 19(2).

The Information Technology Act 2000 after its amendment in 2008 has provided for such reasonable restrictions. These are in the form of powers granted to central or state Governments to issue directions for interception, monitoring or decryption of any information through any computer source located in India.

Offensive speech against women-

The advent of the internet has expanded the reach of freedom of expression for millions of internet users. Information wants to be free and the internet fosters speech and expression for providing basic right. In Neelam Mahajan Singh V. Commissioner of Police on the question of the balance between freedom of speech and expression and public decency it was held: —'We need not to attempt to bowdlerize all literate and thus rob speech and expression. A balance should be maintained between freedom of speech and expression and public decency and morality but when the latters is substantially transgressed the former must give way.'

Ritu Kohli Case- The perfectly normal married life of Ritu Kohli, New Delhi turned upside down, when she started receiving a number of emails from an unknown source. Initially she ignored the mails. Stalker used obscene and obnoxious language, and post her residence telephone number and other personal details on various websites, inviting people to chat with her on the phone. As a result, she started receiving numerous obscene calls at odd hours from everywhere, then she got alarmed. Distraught, Kohli lodged a police complaint. Fortunately Delhi police immediately sprang into action. They traced down the IP address (Internet Protocol address) of the hacker to a cyber cafe. The cyber stalker- Manish Kathuria, later got arrested by the Delhi police and was booked under sec 509 of the IPC (Indian Penal Code) for outraging the modesty of a woman and also under the IT Act (Information Technology Act) of 2000. The case highlighted here is the first case of cyber stalking to be reported in India.

CONCLUSION AND RECOMMENDATIONS:

The IT (Amendment) Act, 2008 has reduced the penalties that are quantum of the punishment for most cyber crimes. This needs to be taken into consideration. Most cybercrimes should be made a non-bailable offence. A comprehensive data protection system must be included in the law to make it more effective. Provision under Section 66A of the IT Act goes beyond reasonable restrictions on freedom of speech and expression under the Constitution of India. They must be removed to make the supplies legally sustainable. The government should strive for bilateral cooperation with other countries to exchange information on cybercrime. Social media platforms must strengthen their privacy practices to control crime against marginalized sexualities or genders. Online platforms may also hire local staff, such as grievance or appeal officers based on local language and culture. The government must ensure effective functioning of prevention of cybercrimes against women and children. The privacy of the complainant must also be protected.

Under the Indian criminal justice system, there is a strict criminal procedure against those accused of committing such heinous crime, but there is no mechanism for the victim to demand that the obscene photos be removed from the online platform. There are no provisions in the IPC and IT act based on women's experiences. Procedural obstacles also hinder women's rights. Once the photos are posted on an international porn site, there is no mechanism in India to remove those photos or videos. The woman is aware of the use of online platforms, but does not know what to do about the difficult situation and cybercrimes. Women should be careful before publishing photos or videos of themselves or to their loved

ones, at least they shall provide a password to the online material they are willing to publish. Changing the password periodically will help to protect.

References

1. ''Crime in India'' Report by National Crime Record Bureau in year 2019
2. Dhruti M Kapadia ,Cyber Crimes Against Women And Laws In India , (Feb 26,2019, 04:43 PM) https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/.
3. "Text Book On Cyber Law" by Dr.Bhagyashree A. Deshpande- Central law Publications Page no – 108
4. Article published by Sandhya Keelery on www.statist.com on cyber stocking and bulling cases reported in India 2019 – Published on 25.02.2021
5. Tiwari; Garima, Understanding Laws Cyber Laws & Cyber Crimes (Lexis Nexis Publication), 2014, Pg no. 8
6. https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html
7. https://gethackingsecurity.wordpress.com/2012/06/25/cyber-crime-history-and-evolution/
8. https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/
9. https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/
10. Cyber Crime Against Women: Right to Privacy and Other Issues, Sanjeev Kumar & Priyanka Journal Of Legal Studies and Research Volume 5 Issue 5, Oct 2019
11. The Information Technology Act,2000 notified on 17thOctober, 2000 with 94 sections divided into 13 chapters and 4 schedules
12. "Crimes Against Women along with Women Empowerment Laws" by Dr. Surinder Mediratta – Delhi Law House - year 2009- Page no. 1
13. Article 14, 15, 15(3),16, 39(a), 39(b),39(c),42 of the Constitution of India
14. Justice K. S. Puttaswamy vs Union Of India (2017) 10 SCC 1
15. Ibid
16. Universal Declaration of Human Rights – Article 12
17. 2015 SC 1523
18. (1998) 8 SCC 296
19. See also, Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd. and Ors. 2019(175) DRJ 66.; High Court of Gujarat in Dharamraj Bhanushankar Dave v. State of Gujarat & Ors.,; Supreme Court of India in the case of K.S. Puttaswamy v. Union of India.
20. (2017) 10 SCC 1
21. Definition of Dignity by Cambridge Dictionary.
22. Pavan Duggal -'Cyber Law'- Second Edition- LexisNexis- year 2020 Pg. No. 20
23. 1996 CrLJ 2725