CYBER CRIME AGAINST WOMEN: RIGHT TO PRIVACY AND OTHER ISSUES

Written by ***Sanjeev Kumar* & Priyanka*****

** Assistant Professor Law, Career Point University, Hamirpur, HP*

*** LLM From Career Point University, Hamirpur, HP*

ABSTRACT

Though crime against women is on a rise in all fields being a victim of cybercrime could be most traumatic experience for a woman. Especially in India where the society looks down upon the women and the law doesn't even properly recognize cybercrimes. In this paper I plan to discuss upon the various types of cybercrimes that can be inflicted upon a woman and how they adversely affect her. I shall also briefly examine upon the various laws that exist to protect women in such cases such as the Information Technology Act (2000) and the constitutional liability. I will be taking assistance of various cases reputed cases (eg: Ritu Kohli case) in cybercrime to arrive at our conclusion. We are also having an elaborate review upon the recent increase in cybercrime on women and its various causes. Right to privacy is coming under the expended ambit of article 21 of Indian constitution. So whenever there is some cyber crime which is related to the persons private property or its personal stuff then the accused can be charged of violation of article 21 of Indian constitution, and prescribed remedy can be invoked against the accused. I also plan to suggest several remedies to counter the ever increasing cybercrime against women in India. At our conclusion we will focus upon the options available to the victims to cybercrime and the changes required in legal system to effectively curb the rising spirits of cyber criminals.

Keywords: *Cybercrime, India, Women, Crime against women, Right to privacy*

INTRODUCTION

The traditional Indian society places women in a very high regards, the Vedas glorified women as the mother, the creator, one who gives life and worshipped her as a 'Devi' or Goddess. The women occupied a vital role and as such her subjugation and mistreatment were looked upon as demeaning to not only the woman but towards the whole society. However, in modern times women are viewed and portrayed as sex objects, she is treated inferior to men in various societal spheres and functions; this has created a huge gender bias between the men and women where even the men think that their wrongdoings towards women cannot be penalized. Cybercrime and internet bullying works in similar manner where the wrong-doers are not afraid of any authority that can penalize. The cyber world in itself has a virtual reality where anyone can hide or even fake his identity, this gift of internet is used by the criminally minded to commit wrongful acts and then hide under the blanket provided by the internet.

Digital India is the gist of many innovations and technological growth. More than half population are in the routine of using Computer, internet and other devices which are most commonly used are social media sites such as Facebook, chat rooms, Instagram, skype, WhatsApp, Dating sites etc. At one side of the coin the digitalization has strengthen the system of India in all terms such as education, economy, governance etc., but at the other side it brought cyber-crimes also in India at very large number. Crime is a social and economic phenomenon and is as old as the human civilization. Crime is basically a legal concept and also has the section of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment". Crime, in whatever manner it is, it directly or indirectly, always affects the society. Due to the continuance increase in the use of computer, internet, numbers of new crimes have emerged and those crimes are basically termed as cyber crimes. These crimes may target any group of society, but women are the most targeted group. In Indian society women are the real victim of cyber crimes.

CONCEPT OF CYBER CRIME

The term cyber crime is nowhere defined, this concept is varied because the crime which is going to committed by using any means of communication or internet can be termed as a cyber

crime. To understand the concept of cyber crime, it is necessary to see the concept of crime, which is, attach with the computer and internet. The concept of cyber crime is not radical different from the concept of conventional crime. Both include the conduct whether act or omission which causes breach of rules of law and counterbalance by the state.[i]

Cyber crime may say to be those species of which genus is the conventional crime and whether the computer is either an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crime come within the ambit of cyber crime.[ii]

CYBER CRIME AGAINST WOMEN

Now a day's cyber crime against women is very familiar issue. Every second, one woman in India gets trapped to be a victim of cyber crimes and the online podiums are now the new platform where a woman's privacy, dignity and security is more and more being challenged every moment. Technology is the resource used by some criminals who target to defame women by sending obscene e-mail, WhatsApp messages, stalking women by using websites, chat rooms, and worst of all by developing pornographic videos, mostly created without their consent, spoofing e-mails, morphing of images for pornographic content by using various software's available online.

Indian women are not able to report cyber crimes immediately as they are not really aware as to where to report such crimes or they are not serious about reporting the same due to social embarrassment they don't want to face. In cyber crimes against women, the effect is more mental than physical while the focus of the laws ensuring women's security is more on physical than mental harm. In this one can say that the mindset of women especially needs to broaden and they must be the whip to curb down by taking derring-do against such criminals that is to go ahead and lodge an immediate complaint. Most of the problems can be solved if women report the crime immediately and warn the abuser about taking strong legal action.[iii]

Cyber-criminals use computer technology to access personal information and use internet for harassment and exploitation purposes which includes stalking, blackmailing, threatening via

emails, photo morphing, cyber pornography etc. Now-a-days, perpetrators are gradually misusing Cyber platforms to harass and abuse women for curious pleasures in India. Women are mostly targeted for cyber stalking, harassment, extortion, blackmail, etc. The Women often trust criminals or abuser and share their personal information which results numerous cybercrimes. Many times, perpetrators get a chance to harass, abuse, blackmail etc. the woman and children more because they are unaware about the procedure of filing a complaint. Cyber crimes against women incept generally through fake Ids created on Facebook, Twitter and other social media platforms causing grave harm to women, as through these platforms, major blackmailing, threatening, bullying, or cheating via messenger messages and email are done by perpetrators. Ill-intentioned men perpetrate these cyber-crimes with malafide intention such as illegal gain, revenge, insult to the modesty of a woman, extortion, blackmailing, sexual exploitation, defamation, incite hate against the community, prank satisfaction of gaining control and to steal information.[iv]

SOME MAJOR CYBER CRIME AGAINST WOMEN

Some of the major well-known cyber crimes have put thousands of women into various health issues such as depression, hypertension and women suffer from anxiety, heart disease, diabetic and thyroid ailments due to eharassment. Major Cyber crimes are as under:

Cyber stalking; cyber stalking is on the rise and women are the most likely targets. Cyberstalking is a way to use the Internet to stalk someone for online harassment and online abuse. A cyberstalker does not engage in direct physical threat to a victim but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation.[v]

Harassment through e-mails; Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via email. E-Harassment is similar to the letter harassment but creates problem quite often when posted from fake ids.[vi]

Defamation; Cyber defamation includes both libel and defamation. It involves publishing defamatory information about the person on a website or circulating it among the social and friends circle of victims or organisation which is an easy method to ruin a women's reputation by causing her grievous mental agony and pain.[vii]

E- Mail spoofing; it generally refers to an e-mail that emerges from one source but has been sent from another source. It can cause monetary damage.[viii]

Phishing; Phishing is the attempt to gain sensitive information such as username and password and intent to gain personal information.[ix]

Morphing; Morphing is editing the original picture by unauthorised user or fake identity. it was identified that female's pictures are downloaded by fake users and again re-posted /uploaded on different websites by cresting fake profiles after editing it.[x]

Trolling; Trolls spreads conflict on the Internet, criminal's starts quarrelling or upsetting victim by posting inflammatory or off-topic messages in an online community with the intention to provoke victims into an emotional, upsetting response. Trolls are professional abusers who, by creating and using fake ids on social media, create a cold war atmosphere in the cyber space and are not even easy to trace.[xi]

Cyber Pornography; Cyber Pornography is the other threat to the female netizens. This would include pornographic websites; pornographic magazines produced using computers and the internet.[xii]

REASONS FOR THE GROWTH OF CYBER CRIME AGAINST WOMEN IN INDIA

The reasons for the increasing cyber crime rate against women can be categorised into two folds: legal and sociological reasons. As this is very much clear that the 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 etc give special protection to women , but the same protection seems not to be given in general under the specific statute. On the other hand, most

of the cyber crimes remained unreported due to various other reasons such as hesitation and shyness of the victim and her fear of defamation of family's name. Many time such victims feels that she herself is responsible for the crime done to her.

Legal Reasons

The objective of the IT Act is crystal clear from its preamble which confirms that it was formed largely for improving e-commerce hence it covers commercial or economic crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unacquainted with the protection of net users. As we deliberated above that majority of cybercrimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmitting obscene material in electronic form), 72(breach of confidentiality). The most of the cybercrimes other than ecommerce related crime are being dealt with these three sections. Cyber defamation, cyber defamation, email spoofing, cybersex, hacking and trespassing into one's privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions11. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 509 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. Indian constitution guarantees equal right to live, education, health, food and work to women, however until recently there were no specific penal provisions protecting women specifically against internet crimes. Ever since the 2012 Delhi Gang Rape case (Nirbhaya Case) there has been a huge outcry over bringing out new reforms and penal provisions so as to protect women against the criminally minded. The 2013 Criminal Law Amendment Ordinance contains several additions to the Indian Penal Code, such as to sections 354, 354 A, 354 B, 354 C & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner. As it has been discussed earlier that transcendental nature of Internet is one of the main reasons for the growth of cybercrime so whereas Section 75 of the IT Act deals with the offences or contravention committed outside India but it is not talking about the jurisdiction of the crimes committed in the cyberspace specially the question of place for reporting the case arises when the crime is committed in one place affected at another place and then reported at another place. Although in the most of the cases, for the matter of territorial jurisdiction Criminal Procedure Code is being followed.

Sociological reasons

Most of the cybercrimes remain unreported due to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times, she considers that she herself is accountable for the crime done to her. The women are more vulnerable to the danger of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women fear that reporting the crime might make their family life difficult for them; they also question whether or not they will get the support of their family and friends and what the impression of society will be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher.

WHAT VICTIMS NEED TO DO

Unfortunately even today the Indian police tends to not tends to take cybercrimes seriously, in such scenario, the woman or the young girl who falls prey to cyber victimization should first contact a women assistance cell or NGO (such as All India Women's Conference, Sakshi, Navjyoti, Centre for cyber victims counselling) which will assist and guide them through the process, also this will make sure that police does not take any case lightly.

THE LEGAL FRAMEWORK FOR THE PREVENTION OF CYBER CRIME AGAINST WOMEN

The internet mainly has two unique characteristics. Firstly, it transcends physical / geographical barriers, and hence, the abuser may be acting from any part of the world. Secondly, the internet extends anonymity to the users.[xiii] Essentially; there are two major laws in India that address cyber- crimes against women to a large extent- The Indian Penal Code and the Information Technology Act. The IPC is a general criminal law of the land, which defines a large number of offences, and prescribes punishment for the same. Unlike the IPC, the IT Act is a Specific Law dealing with the many aspects of the use of information technology, including the

commission of crimes.[xiv] Under the Information and Technology Act, 2000, stalkers and cybercriminals can be booked under several sections for breaching of privacy:

Section 66A: Sending offensive messages through communication service, causing annoyance etc., through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine.[xv]

Section 66B: Dishonestly receiving stolen computer resource or communication device with punishment up to three years or one lakh rupees as fine or both.[xvi]

Section 66C: Electronic signature or other identity theft like using others' password or electronic signature etc.[xvii]

Section 66D: Cheating by person on using computer resource or a communication device shall be punished with imprisonment of either description for a term which extends to three years and shall also be liable to fine which may extend to one lakh rupee.[xviii]

Section 66E: Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.[xix]

Section 66F: Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization.[xx]

Section 67 deals with publishing or transmitting obscene material in electronic form. The earlier section in ITA was later widened as per ITAAct, 2008 in which child pornography and retention of records by intermediaries were all included.[xxi]

Section 72: Punishment for breaching privacy and confidentiality diaries were all included.[xxii]

Section 354D: This section deals with stalking. It defines stalker as a man who follows a woman and tries to contact such woman, monitors every activity undertaken by the woman while using digital media.[xxiii]

CONSTITUTIONAL LIABILITY

Hacking into someone's private property or stealing some one's intellectual work is a complete violation of his right to privacy. The Indian constitution does not specifically provide the "right to privacy" as one of the fundamental rights guaranteed to the Indian citizens but it is protected under IPC.

Right to privacy is an important natural need of every human being as it creates boundaries around an individual where the other person's entry is restricted. The right to privacy prohibits interference or intrusion in others private life. The apex court of India has clearly affirmed in its judicial pronouncements that right to privacy is very much a part of the fundamental right guaranteed under article 21 of the Indian constitution.[xxiv]

Thus, right to privacy is coming under the expended ambit of article 21 of Indian constitution. So whenever there is some cybercrime which is related to the persons private property or its personal stuff then the accused can be charged of violation of article 21 of Indian constitution, and prescribed remedy can be invoked against the accused.

JUDICIAL APPROACH

1. Ritu Kohli case: - Ritu Kohli Case was India's first case of cyber stalking, in this case Mrs. Ritu Kohli complained to police against a person, who was using her identity to chat over the Internet at the website http://www.micro.com/, mostly in Delhi channel for four consecutive days. Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was also deliberately giving her phone number to other chatters encouraging them to call Ritu Kohli at add hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on add hours. The said call created a havoc in personal life of the complainant consequently IP addresses was traced and police investigated the entire matter and ultimately arrested the offender. A case was registered under the section 509, of IPC and thereafter he was released on bail. This is first time when a case of cyber stalking was reported.[xxv]

Similar to the case of email harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the IT Act that perpetrator can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again for outraging the modesty of women

2. State of Tamil Nadu vs. Suhas Katti, in the present case emails were forwarded to the victim who was a divorcee woman for information by accused through false email account opened by him in her name. the posting of messages resulted in mental harassment to the victim as annoying phone calls were coming to her in the brief that was soliciting. She therefore, filed a complaint in the Egmore court in February 2004 and the Chennai police cyber cell arrested the accused. He was filled under Section469/509 IPC and Section 67 of IT Act, 2000. Charges were proved against him and he was booked under the above-mentioned sections.[xxvi]

   One case was reported from Kottayam in Kerala where a girl went to meet with a person she had become on Facebook. However, when she met him, she was abducted. The girl was however traced and later she told the Police that when she met with the boy he had forcibly taken her to a hotel and assaulted her.

PREVENTIVE MEASURE PROVIDED BY GOVERNMENT

A) LEGISLATIVE SUGGESSTIONS

1) Special statutes on cyber crime against women is required to be passed to deal with the all form of cyber crime against women.

2) Statutes and laws made by the legislature related to cyber crime against women must be based on mental harm than the physical harm as till now it is made more on physical harm.

B) JUDICIAL SUGGESSTIONS

Alike various tribunals, a special bench for dealing with cyber crimes against women may be created at least in each and every High Court. Special branch may also be created in every metropolitan cities and districts.

C) SUGGESTIONS TO PROTECT WOMEN FROM GETTING VICTIMIZED TO CYBER CRIME

1) Always use strong passwords and don't share passwords it may sound pointless. As nobody in their right mind shares their password, right? Wrong any person may have shared their password with a trusted friend or partner. While friends may not intentionally cause you harm, they may accidentally reveal your password to someone. Sometimes relationships change before your password does. So, it is very necessary to keep passwords private as well as complicated.

2) Don't always share more than mandatory: Relationships have only two sides in a spectrum – very good or very bad. Even the best of people can also swing from one end of the spectrum to the other. That is why use caution when you share messages, pictures, information or anything that has the potential to come back and embarrass you.

3) Don't meet online friends etc. alone: Always let your parents, friends and family know who you are meeting and where.

4) Don't reveal everything: Always be careful about posting details about your activities etc.

5) Simply block people you don't want to interact with

6) Reporting a cyber crime: This is very important that every woman must report any such cyber crime without any hesitation.

CONCLUSION

The chief problem of cybercrime lies in the modus operandi and the persistence of the cybercriminal. The police, judiciary and the investigative agencies need to stay abreast with the latest developments in web-based applications so that they can quickly identify the actual perpetrator. It is the job of the legal system and regulatory agencies to keep pace with the Technological developments and ensure that newer technologies do not become tools of exploitation and harassment. Governments can take legislative measures that ensure human rights; especially women's rights are protected online just as they are physical spaces.

Legislation should not just protect users; however, it should also educate and inform all groups on how to exercise their communication rights. At the same time, Individuals must become savvy both online and offline; know how to take precautionary measures in cyberspace and how to seek recourse if their rights are violated. Though there used to be several difficulties in dealing with cybercrimes such as loss of evidence and lack of cyber army but with the Criminal law Amendment Bill (2013) most of these problems have been taken care. However, several changes are still needed such as cyber savvy judges. Cybercrimes against women are still taken lightly in India, mostly because in general the respect towards women in our modern society is on a decrease also a lot of people are unable to come to terms with the fact that even posting images of someone online in a crime. Cybercrimes such as morphing, e-mail spoofing do-not have a moral backing in society and hence are taken lightly. This brings us to the most important part where social advancement is needed, people need to recognize the rights of others and realize what constitutes a crime.

They must learn not to interfere with the private lives of others; respect towards women in society needs to increase. All this can only be done if young kinds are taught from a young age to respect women. Hence, to counter cybercrime against women in India, not only stricter penal reforms are needed but also a change in education system is a huge requirement. Such change cannot come from within a single block of society but people, government and NGOs etc. need to work together to bring forth such changes. Women themselves must be trained to take preventive measures, such as caution in posting their and their loved ones' photographs and video clips online, caution in communicating with strangers online, and protecting passwords and other vital information which may compromise with the woman's security and privacy. Women internet users in India required an increased awareness of enhancing privacy settings in social networking sites as a preventive measure. Thus, there is an urgent need of bringing awareness and consciousness among women to be careful while using internet facilities and also a proper guidance if somehow, they face cybercrime then they can raise their voice against it. There is also an alarming requirement for knowledge and technical enhancement for prevention of woman harassment in India.

REFERENCES

[i] Dr. Mrs. K. Sita Manikyam, Cyber Crime – Law and Policy perspectives, 40 (Hind Law House, Pune, 2009).
[ii] Cyber Crimes and the law, Legal India,legalnews and law resource portal (Feb 26,2019,03:21 PM), available at http://www.legalidia.com/cyber-crimes-and-the-law/.
[iii] 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/.
[iv] *Id.* at 6.
[v] Debarati Halder, Cyber Crime Against Women in India, (Feb 26,2019,08:12PM) www.cyberlawtimes.com/articles/103.html.
[vi] *Id.* at 8.
[vii] Shobhna Jeet, Cyber crime against women in India: Information Technology Act, 2000 (Feb 28, 2019,06:43PM) www.elixipublishers.com.
[viii] Nishant Singh, Crime Against Women, 52 (Ancient Publication House, Delhi, 2014).
[ix] *Id.* at 53.
[x] *Id.* at 53.
[xi] *Id*. at 54.
[xii] Sobha Sexna, Crime against women *53,* (Deep and Deep Publication, Delhi, 2014).
[xiii] Ms. Saumya Uma, Outlawing cyber Crimes Against Women in India, Bharti Law Review, April- June, 2017 (Feb 24,2019, 09:16 PM) http://docs.manupatra.in.
[xiv] *Id.*
[xv] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 66A.
[xvi] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 66B.
[xvii] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 66C.
[xviii] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 66D.
[xix] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 66E.
[xx] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 66F.
[xxi] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 67.
[xxii] Information Technology (Amendment) Act, 2008, No 10, (2009) $ 72.
[xxiii] Indian Penal Code, 1860 $ 354D.
[xxiv] INDIA CONST. art. 21.
[xxv] The Hindustan Times, New Delhi dated 23 December 2003 (Fab. 29, 2019, 2: 23PM) www.ijcrt.org>papers>IJCRT1807078.
[xxvi] Decided by Add. CMM , Egmore, Chennai on 5/11/2004 (Fab. 28, 2019, 9: 23PM) www.ijcrt.org>papers>IJCRT1807078.