ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

Cyber Crime against Women in India

Kavita Singh

Assistant Professor, Kotilya Law College, Jaipur.

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 recognise cybercrimes. In this paper I plan to discuss upon the various types of cybercrimes that can be inflicted upon a women 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 new laws that are coming upon in this field such as the Criminal Law Amendment Act 2013. I will be taking assistance of various cases reputed cases (Air Force Balbharati School case (Delhi)) in cybercrime to arrive at our conclusion. We are also having an elaborate review upon the recent increase in cybercrime against women.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.I also plan to suggest to counter the ever increasing cybercrime against women in India.

INTRODUCTION-

Cybercrime is a global phenomenon. With the advent of technology, cybercrime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. Even though India is one of the very few countries to enact IT Act 2000 to combat cybercrimes, issues regarding women still remain untouched in this Act. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. But the grave threat to the security of women in general is not covered fully by this Act. Cyber bullying can affect everyone, including children. Safety Web provides support for parents to improve internet safety for kids.

MEANING OF CYBER CRIME-

The Information Technology Act, 2000 nor defines "cybercrimes" neither uses this expression, but only provides the definition of and punishment for certain offences. Thus two kinds of definition of cybercrimes can be given. In narrow terms cybercrime consists of only those offences which are mentioned under the Information Technology Act,2000, whereas broadly speaking cybercrime can be said to be an act of omission, commission or committed on or through or with the help of internet, whether committed directly or indirectly and which is prohibited by any law for which punishment corporal or monetary is provided. In this context it can be concluded that Information

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

Technology Act, 2000 provides punishment for only certain offences and is not exhaustive of all cybercrimes.

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission. It is an offence that is 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 to the victim directly or indirectly, using modern telecommunication networks such as Internet. Women especially young girls inexperienced in cyber world, who have been newly introduced to the internet and fail to understand the vices of internet, and hence are most susceptible to falling into the bait of cyber criminals & bullies.

Types of cybercrime that are committed against women:

Amongst the various cybercrimes committed against individuals and society at large the crimes which can be mentioned as specially targeting women are as follows: –

1. Cyber pornography-

Of all the crimes committed on the internet pornography appears to be the one having serious moral implications. Being a victim of pornography is the most traumatic experience for a woman. Cyber pornography is the threat to the female citizens. This would include pornographic websites; pornographic magazines produced using computers and the Internet.

Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly called is widespread. Almost websites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs. The new technology is not merely an extension of the existing forms like text, photographs and images. Apart from still pictures and images, full motion video clips and complete movies are also available. Another great disadvantage with a media like this is its easy availability and accessibility to children who can now log on to pornographic websites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present. Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the internet.

[i]It is to be noted that Traditional law of obscenity is contained under sections 292 & 293 of Indian Penal Code, 1860.Section 292 deals with the sale of obscene books and section 293 provides punishment to person dealing in cyber pornography that is accessible to person under twenty years of age with imprisonment up to three years and fine up to two thousand rupees on first conviction and with imprisonment up to seven years and fine up to five thousand rupees on second or subsequent convictions. The IT Act, 2000 was deficient in dealing with obscenity and consist of a single Section 67 dealing with the crime. IT (Amendment) Act, 2008 amended section 67. The combined effect of sections 66-E, 67, 67-A and 67-B obscenity has been brought under the legal regime and child pornography has been separated from mainstream pornography. Section 67[ii] provides that whosoever publishes or transmits obscene material in electronic form shall on first conviction be punished with imprisonment up to three years and fine which may extend up to five lakh rupees and on second or subsequent convictions, imprisonment up to five years and fine up to ten lakh rupees. Section 67-A[iii] deals with mainstream pornography and provides punishment for publishing or transmitting of material containing sexually explicit act, etc in electronic form with

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

imprisonment up to five years and fine up to ten lakh rupees on first conviction and with imprisonment up to seven years and fine up to ten lakh rupees on second and subsequent convictions. Section 67-B[iv] is related to child pornography. This section provides punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form or creates text , digital images, collects, seeks , browses, downloads , advertises, promotes, exchanges or distributes material in electronic form depicting children in sexually explicit act or entices or induces children for online relationship with one or more children or facilitates abusing children online with imprisonment up to five years and fine up to ten lakh rupees on first conviction and imprisonment up to seven years and fine upto ten lakh rupees on second or subsequent conviction. Other acts having an impact on cyber pornography are indecent representation of Women's Act, 1986 and Young Persons (Harmful Publication) Act, 1950.

2.Cyber-stalking-

Cyber-stalking is a myth that if women "just leave" they will be okay. Cyber stalking is a way to continue to maintain rigid control and instill fear into a domestic partner, even when she has already left the relationship. Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & Internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc. It is believed that Over 75% of the victims are female. The motives behind cyber stalking have been divided in to four reasons, namely, for sexual harassment, for obsession for love, for revenge and hate and for ego. Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. Cyber stalkers target and harass their victims via websites, chat rooms Cyber stalking can be categorised as follows: -

- On-line harassment and stalking that continues over the internet.
- On-line harassment and stalking that is carried out off-line. Hereunder stalker attempts to trace the telephone number or residential address of the target. This crime is committed by collecting all the necessary personal information about the target such as his/her name, age, family background, residential address, telephone number, working place, daily retinue etc and put this information on social websites, porn sites pretending as if the victim is himself/herself posting this information and invite people to contact him/her. Generally, stalkers use indecent language to lure people.

Under IT Act, 2000 there is not even a single section exclusively dealing with cyber stalking. Herein computer is merely used as a tool for committing the offence in the sense that the offender might be causing alarm by sending messages via internet to the victim, threatening injury to him, his property or reputation. Section 503[v] Indian Penal Code, 1860 deals the crime of criminal intimidation and provides that whosoever threatens another with any injury to his person, property or reputation or the person, property or reputation of anyone in whom the person is interested or with the 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 he is legally entitled to do , as the means of avoiding the execution of such threat. Cyber stalking is simply criminal intimidation.

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

3.Cyber Defamation-

Cyber tort including libel and defamation is another common crime against women in the net. This occurs when defamation takes place with the help of computers and / or the Internet e.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Defamation is tortuous liability as well as crime and refers to an act of imputing any person with the intent to lower his reputation in the eyes of right-thinking persons of society or cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is nothing else but method of defaming someone with the help of computer or internet. Online mode of defamation is more dangerous than offline mode both quantitatively and qualitatively. With a single click a defamatory statement/ message reaches numerous people and qualitatively defamatory message can be posted as per convenience in a news group such as the lawyer's group. In maximum cases it has been noticed that the purpose of sending defamatory e-mails to the victim is to satisfy the lust of the criminal which may be either for money or satisfying his illegal or unlawful demand or for avenging rivalry and must be published. Section 499[vi] read with section 4[vii] deals with cyber defamation. Section 499 stated that anyone by words intended to be read 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, subject to exceptions provided in the section to defame a person. Section 4[viii] give legal recognition to electronic records. Therefore, if any defamatory information is posted on the internet, such posting would be covered under the section 499 requirement of publication and would amount to cyber defamation.

4.Email spoofing-

A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates. A review in the cyberlawtimes.com shows that India has crossed the danger mark in cybercrime targeting women. Internet Spoofing is a technique which is used for the purpose of gaining unauthorised access to computer, whereby the intruder sends a message to a computer with an Internet Protocol (IP) address indicating that the message is coming from a trusted port. The more common method used by men is to email vulgar photographs of themselves to women, praising their beauty, and asking them for a date or inquiring how much they charge for 'services'. Besides sending explicit messages via e-mail, SMS and chat, many also morph photographs placing the victim's face on another, usually nude, body.

Perpetrators deceive the victim by putting him under the belief that the message received by him is from an authentic source. This is done by link alteration by adding hackers address before the actual address in any e-mail or page that has a request going back to the original site. SMS spoofing is made possible when several mobile operators integrated their network communication within the internet so that anybody could send SMS from the internet using forms at the websites of mobile operators or even through e-mail. To take an example the criminals set up bogus Automated Teller Machines (ATM) in public places or shopping malls asking the user to enter their PIN codes. Once the card gets into the machine, it would malfunction and return the card to the owner. Thus, the criminal gets enough information to copy the victim's card and uses its duplicate to draw money from the ATM. In India there is no legal provision dealing with spoofing as it is not an independent crime and is used as *modus operandi* to commit other crime. The faulty SMS induces the victim to act accordingly and thus, making him pray to some other regular crime. In a sense it can be

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

considered a variation of digital forgery where one attempts to impersonate by sending a false electronic record which though purported to have been made /or signed by the latter person, but in fact it is not so. As the nature of this crime resembles with that of section 463[ix] related to crime of forgery. Examples of spoofed e-mails which are quite common in day-to-day affairs: -

- Fake e-mail from a system administrator requesting the users to change their password to a specified string and threatening to suspend their account if they ignore it.
- E-mail claiming to be from a person with authority asking the customers to send a copy of their password or other sensitive information.
- E-mail from a fake credit card company asking for personal details, credit card number and password to access online account.

5.Harassment via 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-harassments are similar to the letter harassment but creates problem quite often when posted from fake IDs.

The more common method used by men is to email vulgar photographs of themselves to women, praising their beauty, and asking them for a date or inquiring how much they charge for 'services'. Besides sending explicit messages via e-mail, SMS and chat, many also morph photographs - placing the victim's face on another, usually nude, body. According to Borwankar, most cases go unreported because people are "petrified of adverse publicity".

6.Morphing-

Morphing is editing the original picture by unauthorized user or fake identity. It was identified that female's pictures are downloaded by fake users and again re-posted/uploaded on different web-sites by creating fake profiles after editing it. This amounts to violation of I.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC also. The Times of India reported that in October, a Delhi-based beautician told the police that her photograph was flashed on a porno portal along with her mobile number.

Air Force Bal Bharati School case (Delhi)[x] is a recent case comes under this category where a student of the school was teased by all his classmates for having a pockmarked face. He, who is tired of the cruel jokes, decided to get back at his tormentors and scanned photograph of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. The father of one of the class girls featured on the website came to know about this and lodged a complaint with the police. Such acts can be penalised under I.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC sec 509 also.

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

CONCLUSION & SUGGESTION: -

The transcendental jurisdiction of Internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women 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 Criminal Law Amendment Act, 2013 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. No doubt Information technology act, 2000 has been passed by the Indian Parliament with the objective to facilitate to prevent "Cyber Crimes". But the reality is that it is not a separate code for electronic transactions. It has only a gap filling role and it does not provide a separate legal regime and does not cover up the issues that have cropped up by the use of Internet especially cyber stalking, morphing and e-mail spoofing.

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 don't 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 recognise the rights of others and realise what constitutes a crime.

We 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.

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

ENDNOTES:

[i]

[ii] Section 67 of the Information Technology (Amendment) Act, 2008(10 of 2009)

[iii] Section 32 of the Information Technology (Amendment) Act, 2008(10 of 2009)

[iv] Section 32 of the Information Technology (Amendment) Act, 2008(10 of 2009)

[v] Section 503 of the Indian Penal Code, 1860.

[vi] Section 499 of the Indian Penal Code, 1860

[vii] Section 4 of the Information Technology Act, 2000

[viii] Section 4 of the Information Technology Act, 2000

[ix] Section 463 of Indian penal Code, 1860

[x] Abhimanyu Behera, " Cyber Crimes and Law In India," XXXI,IJCC 19 (2010)