

VICTIMIZATION OF WOMEN IN CYBER SPACE AND AN ANALYSIS OF CYBER LAWS IN INDIA

DR.SHWETA DESHPANDE

Abstract: Information Technology has widened itself over the last two decades. The internet is one of the greatest inventions in the area of communication. With its advent, the whole world has become a global village. It has been a boon to students, lawyers, businessman, doctors, teachers.....and unfortunately to criminals too. Although internet is fast becoming a way of life for millions of people, it is also being transformed into a heaven for criminals. Cybercrimes against women are constantly on the raise and women have been drastically victimized in the cyber space. Cybercrimes which can be specially targeted against women include sending obscene e-mails, stalking women by using chat rooms, websites etc, developing pornographic images, e-mail spoofing etc. Internet specially the social networking websites have become haven for offenders to victimize women, the most vulnerable targets, after children. This paper examines the various types of cybercrimes that can be committed against women in the cyberspace, the reasons behind victimization, and how these crimes can be combated through legal means. In this regard the cyber laws prevailing in India to protect them against cybercrimes is discussed in detail.

Keywords: Cyberspace, cybercrime, victimization, cyber stalking, e-mail spoofing, pornography

Introduction: There has been a tremendous growth in information technology over the past two decades and internet is one of the greatest inventions in the area of communication. Originally the Internet served to interconnect laboratories engaged in government research, but since 1994 it has been expanded to serve millions of users and a multitude of purposes in all parts of the world. It has created a virtual world with no boundaries, with the result that people now have an ample of opportunities to ameliorate both personal and professional relationships across borders. The Internet, as no other communication medium, has given an International in other words a "Globalized" dimension to the world. Internet has become the universal source of information for millions of people, at home, at school, and at work. One of the benefits which internet has provided to every section of society is empowerment, including women. With a very low investment, anyone can have a web page in Internet. This way, almost any business can reach a very large market, directly, fast and economically, no matter the size or location of the business. With a very low investment, almost anybody who can read and write can have access and a presence in the World Wide Web. The cyberspace with its enormous benefits has been a boon to human civilization. However the cyberspace has its dark side too. Any technological development is capable of beneficial uses as well as misuse. The cyberspace has become a haven for cybercriminals to victimize women who are the most venerable targets, after children.

In this research paper a detailed analysis of online victimization of women is made and various forms of cybercrimes which can be committed against a women is discussed along with cases and various

judicial decisions. Various provisions of cyber laws to combat cyber crimes is critically analyzed and suggestions are made to curb this menace against women more effectively and efficiently.

Conceptual analysis of the term "Cyber Crime" and various types of cyber crimes that can be committed against women: Computer or cyber crime is a crime where a computer is used as a tool, a target, and an associate to commit the offence. It is a criminal activity directly related to the illegal use of computer and a network, for unauthorized access or theft of stored data that can be used for several criminal activities against victim. Cyber crimes though can be committed against any person, property, organization, there are certain specific types which are committed targeting only women due to their vulnerability. Such categories of cyber crimes include-

Cyber Stalking: In very general terms, stalking refers to harassing or threatening behavior that an individual engages in, repeatedly towards another person. Cyber Stalking refers to the use of internet, e-mail, or other electronic communication devices to stalk/harass another person. Cyber stalkers may operate and adopt any of the following method with a desire to control victim's life-

- They collect nearly all information about the victim such as name, family background, telephone numbers, daily routine of the victim, address of residence/workplace, date of birth etc.
- The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call or using obscene language to invite interested persons

- Some stalkers subscribe the e-mail account of the victim to innumerable pornographic sites and the victim starts receiving unsolicited e-mails
- The stalker can make third party to harass the victim
- Follow their victim from board to board
- Stalkers may send threatening, loving, e-mails and ask for unwanted favours. He may many a times use multiple names when contacting the victim.
- Stalker may also use victims telephone number to harass or to threaten

It is true that both men and women can be stalked on line, but statistics show that the majority of victims are female, especially the age group of 16-35. Over 75% are female victims. More than one million women are stalked online annually in United States.

Ritu Kohli's case- it is the first case in India dealing with cyber stalking. Recently, the Delhi Police arrested **Manish Kathuria** the culprit of the case. In the said case, Manish was stalking a person called Ritu Kohli on the Net by illegally chatting on the website www.mirc.com with the name of Ritu Kohli. Manish was regularly chatting under the identity of Ritu Kohli on the said Website, using obscene and obnoxious language, was distributing her residence telephone number and inviting chatters to chat with her on telephone. Consequently Ritu Kohli was getting obscene calls from different chatters from various parts of India and abroad. Ritu Kohli reported the matter to the police and the Delhi Police swung into action. The police registered the case under the Indian Penal Code for outraging the modesty of Ritu Kohli and after this case various amendments were made to the Information Technology Act to punish the cyber stalkers.

Cyber pornography – ‘obscene’ or ‘pornographic’ material is one that “tends to deprave and corrupt persons”, making such material subject to regulation. Cyber pornography is the act of using cyber space to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting women and children engaged in sexual acts. Indian Penal Code and Information Technology Act explain cyber ‘obscenity’ to mean “anything which is lascivious or appeals to the prurient interest or if its effect is to tend to deprave and corrupt persons”.

Pornography is a major threat to female netizens. Cyber porn and victimization of women of this type of crime is widespread. About 50% of the websites exhibit pornographic material on the internet today. Pornographic materials can be produced more quickly and cheaply on new media like hard disks, floppy disks, and CD-ROMs. The new technology is not merely an extension of existing forms like text, photographs and images. Apart from still pictures

and images, full motion video clips and complete movies are also available.

Air force Bal Bharati School case- A student of the Air force Bal Bharati School, Delhi was teased by all his classmates for having a pockmarked face. To take revenge, he scanned photographs of some girls of his class and teachers morphed them with nude photographs and put them up on a website that he uploaded on to a free webhosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with police that an action was taken

E-Mail 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. E-mail spoofing is a very common way of scamming online. It is a fraudulent e-mail activity in which the sender's address and other parts of the e-mail header are altered to appear as though the e-mail originated from a known or authorized source. By changing certain properties of the e-mail, such as its header, from, Return-path and Reply To fields etc, hostile users can make the email appear to be from some other than actual sender. E-Mail spoofing is possible because the main protocol used in sending e-mail does not allow an authentication mechanism. To illustrate, Pooja has an e-mail address pooja@asianlaws.org. Her ex boy friend, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her image may be spoiled in the eyes of her kith and kin.

Cyber Morphing: Morphing is editing the original picture by an unauthorized user. Such user with fake identity downloads victim's pictures and then uploads or reloads them after editing those pictures. There are so many softwares that provide facility of alteration, modification and edition a photograph like Adobe Photoshop, CorelDraw etc. Most often it is used to depict one person turning into another through technological means or as a part of fantasy or surreal sequence.

In a recent case uploading photos on social networking site Facebook landed a 19 year old girl from Haryana's Fatehabad town in a serious trouble after a youth downloaded one of her pictures and morphed it. The youth Gautam Kumar, later allegedly started blackmailing the girl. The girl alleged that she was abducted by Gautam Kumar, a resident of Sirsa, with the help of his friends Sonu and Raju. Later a complaint was lodged and they were booked under various section of IPC. This type of technique is called as image morphing.

Cyber Defamation – Defamation is the injury that is caused to reputation of a person in the eyes of third person/society. Cyber defamation is publishing of defamatory material against another person with the

help of computers or internet. Although this can happen to both genders, again rate of commission of this crime is more on women. In ***State of Tamil Nadu v. Suhas Katti***, the accused Katti posted obscene, defamatory messages about a divorced woman in the yahoo message group and advertised her as a solicitor for sex. This case is the first defamatory case to be booked under IT Act. He was convicted under various sections of IPC and section 67 of IT Act and was punished for 2 years rigorous imprisonment and fine. Cyber defamation not only lowers the reputation of a person but it may also affect his/her jobs and in case of young girls, many cases reveal that it affects the prospective marriages. Married life of a woman may be turned upside down in cases of cyber defamation. Women may also be subjected to blackmailing in such cases.

Cyber bullying: Cyber bullying means the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. The main aim behind such crime may be to defame the target out of anger, hatred or frustration or secondly when the perpetrator wants to make simple fun of his friends, classmates, or unknown net friends. Globally, India is third behind China and Singapore in cyber bullying and reportedly cases of suicides linked to cyber bullying have grown over past decade.

In a recent incident, Harini a 12 year old girl had put up a profile picture on a social networking site. Her neighbour started bullying her and threatening to misuse information and her photos. Luckily she revealed this to her parents who could take an action against him with the help of cyber crime police.

Harassment via E-Mail: Harassment via email is a form of harassment, which includes black mailing, threatening, and constant sending of love letters in anonymous names or regular sending of embracing mails to one's mail box. Women are the soft targets for this type of crime.

Combating the cyber crimes: Statutory provisions under Information Technology Act: The Government of India enacted Information Technology Act 2000 with the objective to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies. The Information Technology Act was further amended in the year 2008. As far as the above discussed cyber crimes are concerned the following sections of the Act are applicable.

Section 66 of the Act states that 'If a person with the intent to cause or knowing that he is likely to cause

wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack'. The relevant sub sections deal with cyber crimes.

- Section 66 C - If a person fraudulently uses the pass word or other unique identification of another person to commit crime then imprisonment may be upto three years, or/and with fine upto 1,00,000
- Section 66 D - If a person cheats someone using a computer resource or communication, the imprisonment will be upto three years, or/and with fine upto 1,00,000
- Section 66 E - If a person publishes, captures, transmits the images of private parts without his/her consent then he may be punished with imprisonment upto three years or/and with fine upto 2,00,000.

Jawaharlal Nehru University MMS scandal: In a severe shock to the prestigious and renowned institute - Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university. Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market.

- Section 67- Publishing information which is obscene in electronic form attracts imprisonment upto five years, or/and fine upto 10,00,000
- Section 67 A - If a person publishes or transmits images containing a sexually explicit act or conduct then he may be punished upto seven years, and/or with fine upto 10,00,000
- Section 67B - Punishment for publishing or transmitting of material depicting children in sexually explicit act etc on electronic form ie for child pornography, the punishment is upto five years, or/and with fine upto 10,00,000 on first conviction and imprisonment upto seven years, or/and with fine upto 10,00,000 on second conviction.

Apart from the above provisions section 43 can be applied for morphing and e-mail spoofing which penalizes for damage to computer, computer system etc

Cyber Crimes under Indian Penal Code:

- Sending threatening messages by e-mail-section 503. For the offence of criminal intimidation, the offender will be punished with imprisonment of either description for a term which may extend to two years, or fine, or with both.
- Sending defamatory messages-Section 499. The punishment is simple imprisonment for a term

which may extend to two years, or fine or with both.

- E-mail spoofing-section 463-Punishment is imprisonment of two years, or fine or with both.
- Sale, etc of obscene books and printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail -Section 292 and 292A-The offender will be punished with two years imprisonment, or with fine of rupees one thousand or with both. On second conviction the imprisonment will extend upto five years and the fine upto five thousand rupees.
- Sale of obscene objects to young persons-Section 293-for violation of this section the punishment is imprisonment upto seven years and fine which may extend upto seven thousand rupees
- Doing or composing writing etc of obscene songs-Section 294-imprisonment for a term which may extend upto three months, or with fine or with both
- Outraging the modesty of women-Section 509-the miscrenant will be punished with an imprisonment which may extend upto on year or fine or with both.

Procedure for filing a complaint: The complaint regarding commission of cyber crime can be made to the in charge of the of the cyber crime cells which are present almost in every city. The following documents are required to be submitted-

In case of hacking-

- a) Server logs
 - b) copy of defaced web page
 - c) Access control detail mechanisms
 - d) list of suspects
 - e) any other information as required for investigation
- Further in case of e-mail abuse, vulgar e-mail etc, the following information should be provided-
 - Extract of the extended headers of offending e-mail along with the soft copy and hard copy the offending e-mail.

- It is advisable to the victim not to delete the offending email from the mailbox and als,o save the copy of offending email on the computer's hard drive. Thus a little awareness on part of the victim can help the police in investigating the matter more quickly and efficiency.

Conclusion and Suggestions: From the above discussion it can be concluded that, the technology can be abused to victimize women online. The basic problem is although female netizens might know the operations of computers, but still there is lack of awareness/partial computer knowledge about protecting themselves, from being victims. After the commission of the crime most of the women especially Indian female netizens are still not open to immediately report the cyber abuse or cyber crime. In large number of cases, women are unaware of the legal remedies available to them. Existence of cyber crime cells which would help in speedy investigation is many a times not known to them

Following suggestions are made in this regard.

- Government must take measures for mass education and awareness about legal provisions to combat cyber crime amongst women.
- Female netizens should avoid disclosing the personal information to strangers via e-mail or while chatting and avoid sending of photographs to strangers
- Its better not to send the credit card number to any site which is not secured
- For female children, parents should always keep on watch on the sites which their children are accessing.

Undoubtly, commission of cyber crimes against women are raising and since it cannot be stopped in totality its always better to take preventive measures. Also the women victims should immediately report the cyber crime committed against them to the concerned authority so that the offender can be quickly caught and punished.

References:

1. A Moore, Cyber stalking and Women, Facts and Statistics, retrieved from <http://womenissues.about.com/od/violenceagainstwomen/a/cyberstalkingfs.htm>. on 26-12-2015
2. Section 509 of IPC
3. Section 66A IT Amendment Act, 2008.
4. Obscene Publications act of United Kingdom.
5. Section 292 of IPC.
6. Section 67 of IT Act.
7. Lascivious is something that tends to excite lust.
8. Prudent interest is characterized by lustful thoughts.
9. Agarwal Nidhi and Dr.Kaushik Nemaaj, cyber crimes against women, retrieved from www.publishingindia.com/Getbroucher.aspx?query...
10. Eliciting an eye on cyber crime through case studies retrieved from www.ifritcc.org on26-12-2015
11. Retrieved from www.navvi.org/cl-editorial-04/suhas-katti-case.htm on27-12-2015
12. Simhan, R, India ranks third in cyber bullying, Business line available on <http://www.thehindubusinessline.com/industry->

-
- and-economy/info-tech/india-ranks-third-in-cyber-bullying/article357392.ece. [http://newsindianexpress.com/cities/bangalorearticle1352590.ece.](http://newsindianexpress.com/cities/bangalorearticle1352590.ece)
13. Indian Express, cyber bullying new-age threat, No.24, 2012, retrieved from

Dr. Shweta Deshpande/ Assistant Professor/
K.P.E.S's Dr.G.M.Patil Law College/ Dharwad/ Karnataka/