Cyber Space – A Tool of Sexual Harassment

K. Shanthi
Guest Lecturer
School of Excellence in Law, The Tamilnadu Dr. Ambedkar Law University, Chennai, India

Abstract— The present era is marked by two things: heavy reliance on technology and virtual space. But behind the interfusion of these two there exists a world of potent threat and risks. These threats and risks are very much latent in nature and mostly the one committing it or the one upon whom it is committed are extremely difficult to be identified. In a Dynamic Technological Era, the whole world is in fingertips of the individual in second's time through the cyber medium popularly known as NET (Internet). Besides having one of the largest numbers of Internet users in the world, India also has some of the highest statistics of sexual harassment globally. Harassment that women face 'offline' - on the streets, at home, or even at the workplace, is now being directed online as well. Although there are various laws that are made for protection of women even in work place but due to lack of proper implementation and interpretation of law, it has not been quite effective in protecting women. This Paper explores gendered dimensions of cybercrimes like adult bullying, cyber stalking, hacking, defamation, morphed pornographic images, and electronic blackmailing designed to inflict intimidation, control, and other harms are frequently committed by perpetrators who, for many reasons, are unlikely to be identified or punished. This paper tries to highlight the condition of women of cyber victimization and tries to identify the legal safeguards available to women against cyber crimes.

Key words: Sexual Harassment, Women, Cyber Crime, Technology

I. INTRODUCTION

There have been numerous technological advancements over the last decade. The Internet is one of the fastest-growing areas of technical infrastructure development in all nations. In the current era of online processing, maximum of the critical information and details are online and prone to cyber threats. Individuals use the internet because they can gather and share information very easily with other individuals no matter where on the globe they are located. In every creation there are both good and bad sides but when a new one is created for the betterment of people the inventor does not think for its evil sides. Any technological development is capable of beneficial uses as well as misuse [Seminar on "Cyber Crimes against Women, 2009]. The growth of the internet has also resulted in the creation and growth of cyber-crime.

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. For the communication purpose, e-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed materials and Internet-based communication and phone services are growing faster than landline communications. These advancements, while of immense benefit for the population, have also brought opportunities for various criminal activities.

The growth of the information society is accompanied by new and serious threats. When internet was invented, inventors did not think for its bad behavior. But the criminal mentality of human psychology started its misuse by using internet as a tool of crime, which gave the birth to "Cyber-crime" and world is facing a huge challenge from these cyber criminals.

Crimes are as old as man himself and computer crimes are as old as computers themselves. People are very reliant on information systems and the Internet making them easy targets for cyber criminals. The number of internet users has grown exponentially over the last twenty years. Cyber-crimes have become rampant in the city [The Hindu, 2011]. Top 10 countries facing cybercrime is shown in Figure 1. Cyber-crime is a major issue facing society today. Cyber-crime is a major issue facing society today.

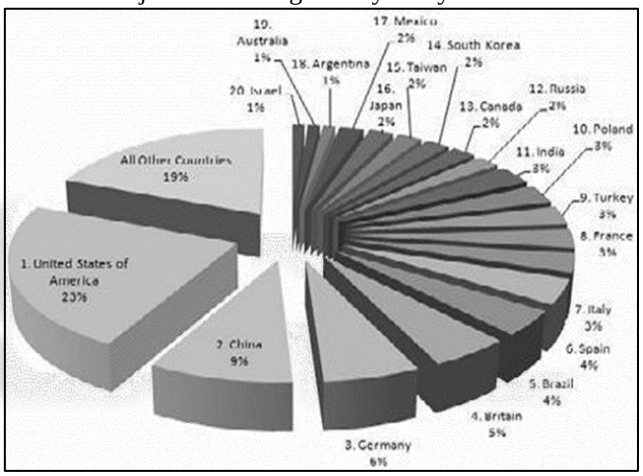

Fig. 1: Cyber Crime: Top 10 Countries
Source: http://www.enigmasoftware.com/top-20-countries-the-most-

With the advent of technology, cyber-crime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. The cyber-crime is the crime, which occurs in the cyber space. In cyber-crime computer is used as a tool, a target, as incidental, and as associate. Cyber-crime also known as computer crime can be defined as -Criminal activity directly related to the illegal use of computer and a network, for unauthorized access or theft of stored or on-line data that can be used for several criminal activities against a victim.

Cyber-Crimes Can Be Broadly Divided into 3 Major Categories – Cyber-crimes against persons, property and Government. Cyber-crimes committed against persons include various crimes like transmission of obscene messages, harassment of any one with the use of a computer such as e-mail, cyber-bullying and cyber-stalking. The second category of Cyber-crimes is that of Cyber-crimes against organization or all forms of property. These crimes include illegal and unauthorized computer trespassing, and transmission of important and critical information outside the organization which can lead to a great loss to the

organization. The third category of Cyber-crimes relate to Cyber-crimes against Government which includes Cyber Terrorism [Duggal].

II. CYBERCRIME AGAINST WOMEN

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances. However, the means that enable the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behavior. The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately women are still defenceless in cyber space.

Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. The widespread circulation of such content is particularly harmful for women. In recent years, there have been numerous reports of women receiving unsolicited emails which often contains obscene and obnoxious language.

India is considered as one of the very few countries to enact IT Act 2000 to combat cyber-crimes; This Act widely covers the commercial and economic crimes. Even then issues regarding women still remain untouched in this Act.

Social Networking and other websites are created and updated for many useful purposes, but they are nowadays also be used to circulate offensive contents also. Individuals who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cybercrime'. Women and minors who post their contact details become especially vulnerable.

As many as 80,000 cyber-crime related complaints have been registered with police in Kerala in 2012, of which 50,000 relate to harassment of women through new hi-tech devices [The Financial Express, 2012].

III. TYPES OF CRIMES

Crime That Are Committed Against Women: Amongst the various cyber-crimes committed against individuals and society at large, crimes that are specifically targeting women are as follows:

1) Cyber-stalking.
2) Harassment via e-mails.
3) Cyber Bullying
4) Morphing.
5) Email spoofing.
6) Cyber Defamation.

A. Cyber Stalking

Cyber Stalking is one of the most widespread net crimes in the modern world. The word "stalking" means "pursuing stealthily". Cyber stalking can be used interchangeably with online harassment and online abuse. It is the use of the Internet or other electronic means to stalk or harass a person. The utilization of technology allows stalkers to harass their target from oceans away.

It involves invading the privacy by following a person's movements across the Internet by posting messages on the bulletin boards, entering the chat-rooms frequented by the victim, constantly bombarding the victim with messages and emails with obscene language.

While Cyber Stalking affects both men and women, women are disproportionately targets, especially of age group of 16-35, who are stalked by men. It is believed that Over 75% of the victims are female. More than one million women and 370,000 men are stalked annually in the United States. An astonishing one in twelve women and one in forty-five men will be stalked in their lifetimes. Statistics of Cyber stalking is depicted in Table 1.

In Cyber Stalking, stalker access the victim's personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim [The Times of India, 2013].

1) 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 posts 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 tracked 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.

2) Another Case

In another case of Cyber Stalking that comes in the notice, a 28 year old woman, Neha Ghai was shocked after she received objectionable calls and text messages on her mobile phones and even vulgar e-mails in her inbox. When she approached the cyber cell and lodged a complaint against the accused, she came to know that she has become a victim of cyber stalking and the stalker had collected all her personal details posted on objectionable portals.

Cyber stalking nowadays become a serious issue and victims should immediately inform the police. The Police can trace the accused by tracking the IP (internet protocol) address of the system that is used for the criminal activity.

B. Harassment via Email

There is no doubt that email has become one of the most heavily used electronic tools of the last decade. Many people send and receive in around 100 emails every day. Harassment on the Internet can take place in a number of ways. One form may include Harassment through e-mails includes blackmailing, threatening, bullying, constant sending of love letters in anonymous names or regular sending of embarrassing mails to one's mail box .

Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cyber-crime. In general they are used to book the perpetrators along with Section 292A of the IPC for printing or publishing

grossly indecent or scurrilous matter or matter intended to blackmail, and under Section 509 of the IPC for uttering any word or making any gesture intended to insult the modesty of a woman.

C. Cyber Bullying

Today, people all over the world have the capability to communicate with each other with just a click of a button and technology opens up new risks.

Cyber bullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. Cyber bullying is "willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature.

Bullying classmates, juniors or even seniors in the school is a common culture among the young school students in India. Social networking sites used in nearly half of cases. Girls are about twice as likely as boys to be victims. With 24 female cases were reported compared with 17 males, reveals that the victims are more often female. India is third on the list behind China and Singapore in the cases of cyber bullying or called online bullying according to a report, highlighting the need to take actions and increase education about online behaviour.

Teens say cruel behavior takes place on-social networking sites as shown in Figure 2 and the states with the highest number of cyber bullying cases in depicted in Table 2.

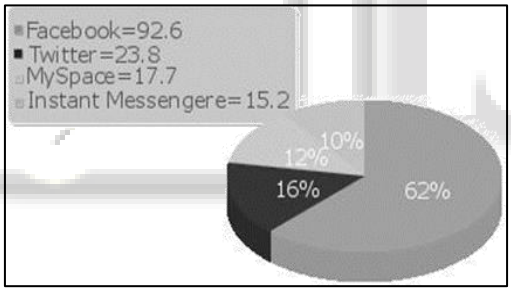

Fig. 2: Cyber Bullying

Source - http://infographicsmania.com/cyberbullying-statistics-2012/

1) Cyber Bullying New - Age Threat

Harini (name changed), a 12 year old girl when put up her profile picture on a social networking site, she did not know that she would soon face serious physical threat. When she finally told her parents about the happening, they were shocked that a person living in the neighborhood had been bullying her and threatening to misuse her personal information and photos if she told anyone. After certain visits to the cyber-crime police station, they somehow managed to get rid of the threat. However, Harini's parents are still not sure how to make their daughter overcome the fear and regain her self-esteem [Indian Express 2012].

D. Morphing

Morphing is editing the original picture by an unauthorized user. When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing. It was observed that female's pictures are downloaded from websites by fake users and again reposted/uploaded on different websites by creating fake profiles after editing them.

This amounts to violation of I.T. Act, 2000. The violator can also be booked under IPC also for criminal trespass under Section 441, Section 290 for committing public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation

E. Email Spoofing

A spoofed e-mail may be said to be one, which misrepresents its origin [Legal India]. It shows its origin to be different from its actual source. E-mail spoofing is a popular way of scamming online. E-mail spoofing is a term used to describe fraudulent email activity in which the sender's address and other parts of the email header are altered to appear as though the email originated from a known or authorized source. By changing certain properties of the email, such as its header, from, Return-Path and Reply To fields etc., hostile users can make the email appear to be from someone other than the actual sender. Email spoofing is possible because the main protocol used in sending email i.e. Simple Mail Transfer Protocol (SMTP), does not allow an authentication mechanism. Email spoof can cause monetary damage also.

F. Cyber Defamation

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

The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person Cyber defamation is publishing of defamatory material against another person with the help of computers or internet.

You build a great brand over 20 years and all it takes is 2 days to destroy it, on the Net [The Times of India 2010]. Unfortunately cyber defamation is not defined by the IT Act 2000 and it is treated by the criminal justice system under the same provisions of publication of obscene materials in the internet.

With the exponential increase in the use of the internet as a medium of communication and sharing of information, chances of use of the web for publication of defamatory content has increased multi-fold and there is a coherent need for a clear law in this area.

1) Laws against Cyber Defamation in India

Abhishek, a teenaged student was arrested by the police in India following a girl's complaint about tarnishing her image in the social networking. Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile. According to Section 67 of the IT Act 2000, any person who sends, by means of a computer resource or any communication device any offensive information, shall be punishable with imprisonment for a term which may extend to three years and with fine. The offence of cyber defamation is well explained in the IPC

under Section 500 which mentions punishment with simple imprisonment that can be extended up to two years or with fine or with both.

2) Some Suggestions & Steps to Tackle Cyber Crimes

Besides, depending on legal system against cybercrimes, women have to be aware of cyber victimization by self, because time has come to reject the acceptance of silent. Moreover cyber laws are not universal, as they vary country to country. Today, every netizen wants to browse web privately and safely especially women. We should take some steps to tackle this problem. Here are some steps and suggestions that how women can save themselves of being victimized in cyber space and how they can make their online perceptions and experiences a safer one, are as follows;

1) Change passwords time to time
   In fact, we all love to have easy-to-remember passwords because, it is simpler. If one wants to lower internet crime risk, changing password is a great way to make personal data and social networks safe and difficult to access for cybercriminal. Baffling or tricky password protect all accounts including cell phones, emails, landlines, banking, credit card etc. and are difficult for anyone to guess. Even, secret questions should not be easily answered. Safest passwords contain letters, numbers and symbols. Avoid words that are in dictionary and any important dates and must use different passwords for different web sites. However, changing password can be very helpful to keep privacy safe.
2) Avoid revealing home address
   This is the rule for women in particular who business professionals are and very visible. They can use work address or a rent private mailbox. Thus, it can help them out in avoiding cyber stalkers. Moreover, women should avoid uploading more material on internet regarding their own information so that no one can easily access them.
3) Maintain stable social relationships
   It is also the fact that we all like to believe that we should have 2000 friends. Dunban's number1 suggests a limit to the number of people, a human being can have a proper social relationship with, and that number is 150. Probably, we don't need those 2000 facebook friends, because we are likely physical unable to really know more than 150 of them. Maintaining a limit on the number of the people will ensure our information is distributed to people who you really know and away from friends-of-friends-of-friends who you actually do not know all too well. Women should make distance from impermissible friendships.
4) Awareness campaign against cybercrimes
   Awareness campaign must be set up from the grass root level such as schools, collages etc. about cybercrimes like stalking cheatings, economic cheatings, defamatory activities, misusing emails and social networking websites, virtual rapes, cyber pornography, email spoofing etc. These campaigns can be fruitful in paralyzing cybercrimes.
5) Seminars and workshops for better understanding of cyber victimization
   Police, Lawyers, social workers, and NGOs must be invited to education institutes, clubs, corporate offices, awareness-campaigns, seminars and workshops to discuss about legalities and illegalities of cyber conduct among adults inclusive of both genders. Reporting of cyber victimization at all levels directly to the police and NGOs working cybercrimes must be encouraged. Secondly, workshops and seminars must be conducted for the police personnel for better understanding of such kinds of victimization and quick responses towards the complaints. Academic and legal experts, NGOs etc. must be invited for such workshops and seminars.
6) Rigid and stringent laws
   India must bring in more rigid and stringent laws for cybercrimes against women in the cyber space. It is evident that present India's Information Technology Act includes only few sections for cybercrime, especially against women, hence to curb cybercrimes, either IT Act must be re-modified or a separate law on cybercrimes should be created. Proper law and order against crimes may lead to create good society.
7) Beware of unsolicited calls and messages
   Woman should avoid unwanted or unsolicited phone calls and massages because cell phone may be monitored. If it happens again and again, you should try to record phone calls of harasser and report to the police. Even, they should download applications from trusted websites. Besides, they should discuss and share the problem regarding cyber harassing with their trusted ones like parents, mates or spouses etc.
8) Understand privacy settings of social network
   Social networks and other online content and service providers all have privacy policies and private settings. One must try to understand privacy policies and adopt privacy settings that help in protecting oneself from any potential risk or online harm. So, we must have the knowledge about privacy settings of social networking.
9) Anti-Virus must always be up to date
   One must keep Anti-virus up to date. According to Fight Cyberstalking, Trojans, worms, and email viruses are common ways for would-be cyber stalker to access one's information. One must make sure that Anti-Virus is up to date to lessen probability that one's PC cannot be attached with a Trojan virus, email virus or worms.
10) Check account regularly
    It is clear that every net user has its own account on network sites. We should regularly check our email, blog or website accounts etc. By doing so, we will be in-touch with our belonging accounts on internet and we can lessen the possibilities of hacking, stalking etc by reviewing our account.
11) Protect data on the move
    In our daily life, we often use public computers in internet cafes etc. You should remember that when you are using internet on public computers, web browsers can keep a record of your passwords and every page you have visited. So, you should not forget to erase your tracks or history on web browsers.
12) Keep firewall turned on
    Firewalls are first line of cyber defence and block connections to unknown or bogus sites and keep away from some kind of viruses and hacker. These firewalls are recommended for single computers and are pre-

packaged on some operating systems or can be purchased for individual computers.

Apart from above given suggestions, women should always be in-touch with valuable information about cybercrimes and should be careful before they click any link on internet. Moreover, educating women can also play a considerable role in preventing crimes.

IV. CONCLUSION

India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes; This Act is widely covered commercial and economic crimes which is clear from the preamble of the IT Act but it is observed that there is no specific provision to protect security of women and children.14 However there are few provisions to cover some of the crimes against women in cyber space under IT Act. The model adopted in USA may be proved a step forward in this direction.

Noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal, "While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law a cybercrime friendly legislation; – a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; ….. a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cybercrime capital of the world…… " Let us not be pessimistic that the existing legislation is cybercriminal friendly or paves the way to increase crimes. Certainly, it does not. It is a commendable piece of legislation, a landmark first step and a remarkable mile-stone in the technological growth of the nation. But let us not be complacent that the existing law would suffice. Let us remember that the criminals always go faster than the investigators and always try to be one step ahead in technology.

REFERENCES

[1] Published On Do Something "11 Facts About Cyber Bullying" Available On Http://Www.Dosomething.Org/Tipsandtools/11-Facts-About-Cyberbullying
[2] Indian Express (2012) "Cyber Bullying New-Age Threat" Indian Express, Nov 24 Available On Http://Newindianexpress.Com/Cities/Bangalore/Article1352590.Ece
[3] Itu (2005) "Understanding Cybercrime: Phenomena, Challenges And Legal Response" Available On Http://Www.Itu.Int/Itud/Cyb/Cybersecurity/Docs/Cybercrime%20legislation%20ev6.Pdf
[4] Mukut (2012) "Cyber Stalking -A "Virtual" Crime With Real Consequences" Available On Http://Worldpulse.Com/Node/61115
[5] Seminar On "Cyber Crimes Against Women"-Public Awareness Meeting (2009) Available On Http://Supremecourtofindia.Nic.In/Speeches/Speeches_2009/Seminar__Cyber_Crimes_Against_Women_1-08-09.Pdf
[6] The Financial Express, July 30 (2012) "Cyber Crimes: Criminals Target Women With Hi-Tech Devices" Available On Http://Www.Financialexpress.Com/Story-Print/981431
[7] The Hindu, May 25 (2011) "Cyber Crimes Against Women On The Rise Available On Http://Www.Thehindu.Com/Todays-Paper/Tp-National/Tpkerala/Cyber-Crimes-Against-Women-On-The-Rise/Article2047032.Ece
[8] The Times Of India, March 18 (2013) "Cyber Stalkers Leave Residents In Web Of Trouble" Available On Http://Articles.Timesofindia.Indiatimes.Com/2013-0318/Ludhiana/37813762_1_Cyber-Stalkers-Cyber-Cell-E-Mail-Account
[9] The Times Of India, Dec 18 (2010) "Cyber Defamation Increasing In India Available On Http://Articles.Timesofindia.Indiatimes.Com/2010-1218/Security/28256203_1_Cyber-Defamation-Blog-Sites-Mega-Housingproject
[10] Nidhi Agarwal & Dr Neeraj Kasuhik "Cyber Crimes against Women" Gjrim Vol. 4, No. 1, June 2014.

