



Computer-Generated Offences Against Women

KEYWORDS

Defamation, Cyber Pornography, Cyber stalking

Dr. P.K.Rana

Reader, M.S.Law College, Cuttack

ABSTRACT *With the growth of e-commerce and adoption of economic liberalization we have noticed the rise of the computer-generated crimes against women which is very difficult to identify perpetrator because of geographical boundaries. Our women are very much search and prone to disclose their optional information and therefore their required to work with safeguards.*

Introduction

The computer-generated crime is a crime committed through modern means of communication like computer and internet. These crimes are called 'white-collar crimes' and can be committed from any place of the Globe and can give effect anywhere in the Globe within fraction of seconds. It results into public damage/grievous personal hurt/defamation/loss of character etc. It is the only crime which has no boundaries and may affect every country. Further it is very difficult to identify the wrong-doer because of vicious web of Net all over the globe. Thus, when any crime is committed with the help of computer technology and using computer as a means to commit crime. It is categorized as cybercrime. Cybercrime encompasses not only those crimes which are committed with the help of computer but also computer related crime such as criminal threats, internet auction, fraud etc.

Cyber Crime has been defined as the act of creating, distributing, altering, stealing, misusing and destroying information through the computer manipulation of Cyberspace: without the use of physical force against the will or the interests of the victim.¹ Cyber crime can even be defined as unlawful act where in the computer is either tool or larger or both.² The computer is generally used as a tool in carrying out criminal activities like financial crimes, sale of illegal article, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking etc. The computer may however be target for unlawful acts such as unauthorized access to computer/computer system/computer networks, theft of information contained in the electronic form, e-mail bombing, data dialing. Trojan attacks, internet time thefts, web jacking etc.

II Cyber Crimes and its various forms

The cyber crimes are committed against individuals, as well as Nation Cyber Crimes against individual affects the individual person. It has been observed that women figure is soft and significant by as targets of cyber crimes. Amongst the various cyber crimes committed against women, main crimes are identified and can be enlisted as under:

Harassment through e-mails;

Cyber-Stalking;

Cyber-pornography;

Defamation;

Morphing;

Email spoofing

Let us discuss these crimes one by one.

Harassment through e-mails is very similar to harassing through letters and includes blackmailing, threatening, bullying and even cheating via mail Harassment are similar to the letter harassment but creates problem quite often when posted from fake ids.

Cyber Stalking – It is one of the most talked about net crimes in the Global world Cyber stalking involves following person's movements across the posting messages (sometimes threatening) on the bulletin boards frequently by the victim with e-mails etc. The main targets in this kind of crime are females, children, emotionally weak in unable etc. It is observed that 75% of the victims are female. Generally the motives behind cyber stalking are sexual harassment, obsession for love, revenge and hate and ego and power trips. The availability of free e-mail and website space, the anonymity provided by these chat rooms and forums contribute to the increase of cyber crimes/cyber stalking.

Cyber-pornography – It is another threat to the female netizens. This generally includes pornographic websites, pornographic magazines produced using computer (to publish and print the material) and the internet to download and transmit pornography pictures, photos, writings etc.

Internet has provided a medium for the facilitation of crimes like pornography Cyber porn is wide spread. Easily available Net centers, reproduction of pornographic materials on C.D. Roms, easy circulation through floppy disk and hard disks helps in percolation of cyber pornography in society. Easy availability and accessibility of pornographic web-sites to children is another threat which again results into increase in cyber porn. It has become rampant on the Internet. It is very difficult to regulate as the concept of morality differs from country to country. Cyber pornography is spoiling the young generation of our country.

Cyber Defamation- The law of defamation is another issue, which arises frequently on the Internet. Defamatory statements can be made on the internet through online

message, e-mails, bulletin boards, chart etc. Cyber defamation happens when defamation taken place with the help of computers or internet. For example: someone publishing defamatory statement of another on a website or sends e-mails containing defamatory information to near and dear ones of that person.

Morphing- It is editing the original picture by unauthorized user or fake identify. Generally in this category of crime, female's pictures are downloaded by fake users and again repost on websites by creating fake profiles after editing it.

Email Spoofing- A spoofed e-mail is one which misrepresents its origin. It show its origin to be different from which actually it originate. E-mail spoofing is the practice of changing one's name in email so that it looks like the email came from other. The intention is misrepresentation. In this type of crime, any kind of damage may because including monetary loss.

III Adoption of Safety Measures

The only alternative available to wise persons is the adoption of safety measures which requires to be practiced by women to avoid happening of cyber crimes against them. The safety measures can be enlisted as under:

One important safety measure is to treat your e-mail address as important private data like a phone number or address and only give it to the people you know and trust online. Even the information regarding your bank account number or any other financial information should not be disclosed to the new person and should not be circulated through internet or mobile.

It is always better to have a spam-filter for your e-mail. Spam is junk mail delivered through e-mail which may some times contains viruses or adult content that is vulgar and inappropriate.

You should be aware of all the requests for personal information if asked for any reason if you are storing personal or private information on your computer. Never provide any such information.

Protect you children from on-line dangers. Parents should teach their children to follow the common sense 'rules of the road' for the internet.

Passwords: One should always use Password. A password prevents the entry of intruders. Even the 'Pass phrases' which are used in place of password provides you security. If possible, keep changing your password and it should also not be given or disclosed to near ones.

Firewalls: Fire walls create 'wall' of protection between a network and possible intruders.³ It prevents information from existing on entering a firms computer of LAN and the Internet. If it is properly figured, it filters all the electronic data packets sent to it from the LAN and the outside connection will pass on only verified electronic data packets.

Encryption: it is kind of safety system in which data is accepted only often decrypt. It refers to any algorithm applied to an electronic record that converts plaintext into cypher text, rendering it meaningless for all except the one who has a key to decrypt it. This technology is used for securing Internet trams actions.⁴

Digital Signature: Digital Signatures safeguard informa-

tion and prevent it from falsification on alteration. These digital signature help in signer authentication, document authentication affirmative acts signifying a signature and efficiency.

IV Legal Protection

There are some provisions in IT Act, 2000 relating to cyber crime and offences against women in India.

For tampering with computer source documents.

For Hacking with computer system.

For publishing information which is obscene in electronic form.

For access to protect system.

For breach of confidentiality and privacy.

For publication for fraudulent purpose.

But all these provisions ore not sufficient and needs to be modified. However, these provisions do not mention any crime specifically as against women and children. Under no section in IT Act, 2000, obscenity personal viewing is an offence. And no where cyber stalking, morphing and email spoofing are mentioned as cyber offences. Further, the shadow areas in procedure are regarding jurisdiction and loss of evidence. Lack of cyber army and cyber savy Judges are other lacunae.⁵ Judiciary plays vital role in sharpening enactments according to the order of the day. Similarly, the threats approaching towards the netizens must be communicated to the public at large and more particularly to women. Cyber Awareness programme must be carried out in the society.

Conclusion

This crime comprises new forms of techniques. It is the crime in which advance technology is used to commit the crime. The technological advancement no doubt helps the mankind but sometimes it gives birth to unwanted things which prove harmful to society. Cyber crime is of such a nature. It does not even respect geographical boundaries. It is committed in cyberspace. It means the cyber criminals do not come face to face and are not physically present at the place where actually crime is manifested. Moreover, the police machinery is not well verse with the technology and are required to get equip with it to curb the commission of cyber crime. Due to unusual feature of this crime, it is difficult to collect evidence and to carry out investigation.

To curb this social menace, all will have to come together. The NGOS, Educational Institutions, Police Department and Women Organisations should take the initiative regarding awareness of cyber crimes . While working on the computers and internet, one must go for the safety measures. Further if something goes wrong, we must immediately report back or even warn the abuser about taking strong action. By using various modes of curbing, cyber crime we can minimize cyber crime against women.

Reference

1. W.w.w. statistics, w.w.w.
2. Nagpal R. what is cyber crime
3. Gary H. Anthes, Oct. 17, 1994 at 14.
4. Bruce Schneies. Applied Cryptography 273-74(1994) computer
5. Ibid. 4.