Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
January to March 2026, E-Journal, Vol. I, Issue LIII (53), ISO 9001:2015 - E2024049304 (QMS)

Cyber-Crimes Prevention Against Women

Sandeep Kumar Dixit*

***Research Scholar (Legal Studies & Research) Barkatullah University, Bhopal (M.P.) INDIA**

Abstract- Any criminal activity that uses a computer either as an instrumentally, target or means for perpetuating further crimes comes within the ambit of cyber crime. The origin of cyber crime is to be found in the growing dependence on computers in modern life. In the present 21st century where everything from microwave ovens and refrigerators to nuclear plants are being run by computer, cyber crime has assumed sinister application. Cyber crime is the latest and perhaps the most complicated problems in the cyber world. Cyber crime may be said to be those species, of which genus is the conventional crime and where either the computer is an object or subject of constituting crime.
Keywords-Pornography, Obsession for love, Revenge & hate.

Meaning of Cyber Crime: A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both". The computer may be used as a tool in these kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in these cases- unauthorized access to computer/ computer system/computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking; theft of computer system, physically damaging the computer system etc.

Cyber crime has been a problem as early as the late 1970's. With the ever-changing technology, cyber crime offenders are right there, keeping up with new ways to attack possible Internet victims: While the Internet can bring purpose and even joy to our technological lives, it .has a way of creating its negative side effects too. 'Computer crime' or 'cybercrime' refers to any crime that involves a computer and a network; where the computers may or may not have played an instrumental part in the commission of a crime: 'Net crime' refers, more precisely, to criminal exploitation of the Internet Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement; child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

On the global level, both governments and non-state actors continue to grow in importance, with the ability to engage in such activities as espionage, financial theft, and other cross-border crimes sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions, with the International Criminal Court among the few addressing this threat. Cyber crimes against women are increasing day by day with the advent of the technology and it is causing a great threat to the security of a person. All over the world, the women are victims of such type of crimes.

Types of Cyber Crimes against Women: Cyber-Stalking 'Cyber stalking' occurs when a person is followed and pursued online. Their privacy is invaded, their every move is watched. It is a form of harassment, and can disrupt the life of the victim and leave her/ him very afraid and threatened. Stalking or being 'followed' is the problem that many people, especially women, are familiar with. Sometimes these problems (harassment & stalking) can occur over the Internet. This is known as cyber stalking. So 'stalking' can be defined as a willful conduct involving repeated or continuing harassment of another individual that actually causes the victim to feel terrorized, frightened, intimidated, threatened, harassed or molested. In Cyber stalking, the internet is used to pursue, harass or contact another in unsolicited fashion. The term can also apply to a "traditional" stalker who uses technology to trace and locate the victim and their movements more easily. A cyber stalker's intent is to harm their intended victim, using the anonymity and untraceable distance of technology. In many situations, the victims can never discover the identity of the cyber stalkers who hurt them, despite their lives being completely upended by the perpetrator. Main' targets of cyber stalking are mostly females, children, emotionally weak or unstable etc. It is believed that over 75% of the victims are female. The motives behind cyber stalking may be:

1. Sexual harassment
2. Obsession for love
3. Revenge and hate
4. Ego and power trips

Cyber stalkers can be categorized into three types: The Common Obsession Cyber Stalker the common obsession stalkers refuse to believe that their relationship is over. Do not be misled by believing such stalkers are harmlessly in love.

The Delusional Cyber Stalker: The next type is of the delusional stalkers. They may be suffering from some mental illness like schizophrenia etc & have a false belief that keeps them tied to their victims. They assume that the victim loves them even though they have never met. A delusional stalker is usually a loner & most often chooses victims who are married woman, a celebrity or doctors, teachers, etc. Those in thenoble & helping professions like doctors, teachers etc. are at often at risk for attracting a delusional stalker. Delusional stalkers are very difficult to shake off.

The Vengeful Cyber Stalker: These cyber stalkers arc angry at their victim due to some minor reason- either real or imagined. Typical examples are disgruntled employees. These stalkers may be stalking to get even & take revenge and believe that "they" have been victimized. Ex-spouses can turn into this type of stalker.

The Delhi Police had registered India's 'First Case of Cyber stalking. One Mrs. Kohli complained to the police against the person who was using her identity to chat over the Internet at the website `**www.mirc.com**' mostly in the 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 in obscene language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call her at odd hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly at odd hours, even from remote places such as Kuwait, Cochin, Bombay and Ahmedabad. The said calls created havoc in the personal life and mental peace of Mrs. Kohli, ultimately she decided to report the matter. Consequently, the IP addresses were traced out and the police investigated the entire matter and ultimately arrested Mr. Manish Kathuria, and a case was registered against him under section 509 of the Indian Penal Code (IPC)

Distinction between conventional and cyber crime: There is apparently no distinction between cyber crime and conventional crime. However on a deep introspection we may say that there exist-3 a fine line of demarcation between the 1.y.) The conventional and cyber crime, which is appreciable. The demarcation lies in involvement of the medium in the cases of cyber crime. The sine qua non for cyber crime is that there should be an involvement, at any stage, of virtual cyber medium.

Harassment through E-Mails: It means the act of harassing a user of the Internet using E-MAIL, usually by sending salacious, abusive, or intrusive messages. It 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. Harassment consists of the intentional crossing of your emotional or physical safety boundaries. The legal definition of 'harassment', according to Black's Law Dictionary, is:

"A course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose" or "Words, gestures, and actions which tend to annoy, alarm and abuse (verbally) another person." Recently email account of the daughter of a legend music maestro was hacked into by an offender and he took control of some very private photographs, stored in the inbox of her email inbox. Her father moved a complaint to Union Home Ministry that his daughter is being blackmailed and threatened via email by some unknown person. Later the complaint was referred to the Delhi Police and the investigation of the case was taken up by Inspector Pawan Kumar under the supervision of ACP Sanjeev Yadav of elite special cell of Delhi Police. The unknownaccused person allegedly blackmailed and threatened the girl via email that he would make some of her photographs public as found in her email inbox, if his demand of 100,000 dollar is not fulfilled by her. The aforesaid officers of elite wing of the Delhi Police, the special cell, did a commendable job. The special cell cops traced the Internet Protocol address (IP address) from which the emails were sent. The IP address can be tracked from the header of the email IDs. The. extortive emails sent by the offender were found to be sent mostly from Gmail account. The police tracked down one of the IP address to a residential address located at Mumbai and nabbed the accused person, whose name came to be known as Junaid Jameel Ahmed Khan who confessed his crime. The cops seized the hard disk of the computer from which the alleged emails were sent, prepared the mirror image of the same and the hard disk was sent to the Forensic Science Laboratory, Hyderabad for further analysis. The cops also seized the passport of the offender through which it was found that the offender was at Dubai on the same date when the extortive emails from Dubai were received by the girl, which clearly corroborates the offence committed by the offender. The police have seized and preserved the crucial digital evidences and other documentary evidences which would prove the guilt of the accused person. The special cell cops registered the case under Section 386 Indian Penal Code which deals with offence of extortion. The maximum punishment for such a crime, if proven guilty, is 10 years' imprisonment. The offence is cognizable and non-bailable. The accused although hacked the email, but the police at the preliminary investigation stage did not invoked Section

66 of the Information Technology Act, because the modus operandi of the offender was not known as how he took control of the private photographs, which during investigation and seizure of the computer become apparent that the same has been copied into his computer by hacking the email ID and then Section 66 IT Act was added. The material evidence seized by the cops proved the involvement .of the offender as the IP address was also traced out to be of his residence.

Cyber Pornography: There is no settled definition of 'pornography' or `obscenity'. Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, but it has been held that a law against obscenity is constitutional.

The Supreme Court has defined 'obscene' as: offensive to modesty or decency; lewd, filthy, repulsive. Section 67 of the IT Act is the most serious Indian law, penalizing cyber pornography. Other Indian laws that deal with pornography include the Indecent Representation of Women (Prohibition) Act and the Indian Penal Code. Section 67 of the IT Act states:

"Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely,having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one Lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two Lakh rupees."

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal. Following are few of the cases in this regard: WI Swiss couple case In Mumbai, a Swiss couple gathered slum children and then forced them to appear for obscene photographs. These photographs were then uploaded to websites, specially designed for pedophiles. The Mumbai police arrested the couple for pornography.

The Arzika case: Pornography and obscene electronic content has continued to engage the attention of the Indian mind. Cases pertaining to online obscenity, although reported in media, often have not been registered. The Arzika case was the first in this regard.

The Air Force Bal Bharti School case: This case demonstrated how Section 67 of the Information Technology Act 2000 could be applicable for obscene content, created by a school going boy.

State of Tamil Naduv. Dr L. Prakash: This was the landmark case in which Dr L. Prakash was sentenced to life imprisonment in a case, pertaining to online obscenity. This case was also landmark in a variety of ways since it demonstrated the resolve of the law enforcement and the judiciary as not to let off the hook one of the very educated and sophisticated professionals of India.

Cyber Defamation: It is a crime conducted in cyberspace, usually through the Internet, with the intention of defaming others. 'Defamation' is injury to the reputation of a person. If a person injures the reputation of another, he does so at his own risk, as in the case of an interference with the property. A man's reputation is his property, and if possible, more valuable than the, other properties. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium. Example: A defamatory article can be published in a newspaper or it can be published on a website. Publishing through a website would amount to cyber defamation.

Internet provides us a very cheap and a quick way of communication. It has made the world a close nit organization. Also, with the growth of social networking sites like orkut, facebook, etc, lot of personal information is shared amongst many people. Therefore, the chances of defamation through internet have become a major threat in today's world. Even if a single defamatory email is forwarded, it becomes very difficult to trace and stop its circulation. Any article published on a website is open for the entire world to read. The damage or losses caused to the victim is very huge, especially if the imputation is intended to harm the business of an individual or a business entity.

Email Spoofing: It is an e-mail activity in which the sender address and other parts of the e-mail header are altered to appear, though the e-mail originated from a different source, because core SMTP doesn't provide any authentication, it is easy to impersonate and forge emails. It is usually fraudulent, but can be legitimate. It is commonly used in spam and phishing e-mails to hide the origin of the e-mail message. By changing certain proper-ties of the e-mail, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. The result is that, although the e-mail appears to come from the address indicated in the From field (found in the e-mail headers), it actually comes from another source.

So we can say, if you receive an UNDELIVERABLE email that you did not send, you are the victim of "Email Spoofing." Email spoofing exists when a user receives email that appears to have originated from one source when it actually was sent from another source. In short, your email address was forged. You did not send it, but it was sent from another computer that has your email address.

Most UNDELIVERABLE emails are sent by computers infected with email-type viruses, such as the KLEZ virus. These viruses infect the computers which do not have virus protection. Once the computer is infected, these viruses scan the address book and the inbox of the infected machine gathering email addresses. After gathering email addresses, the virus generates virus-infected email messages, randomly putting the harvested addresses that it found during its scan into the TO: and FROM: fields of bogus emails. The email may also contain a copy of the virus disguised as an attachment. These viruses act as an SMTP server, that is, they send these emails out when the infected computer is online. These email viruses are smart enough, as they do not use the actual email address of the infected computer. It is very likely that someone who has your email address on their computer got an email-spoofing virus and placed your email address into the FROM field of the bogus email. If the email bounces back, that is, if it is rejected by a receiving email server, it is sent back to your email address rather than to the computer from which it originated.

The more common method used by men is to email vulgar photographs of themselves towomen, 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.

Morphing it is nothing but 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 section 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. A Bollywood actress Ms. Celina Jaitley lodged a police complaint against two websites for allegedly morphing her pictures from a photo shoot that she had walked out a year ago. Apparently the sites have obscenely morphed her pictures to sell their gadgetry.

Unfortunately, not only amongst Indian women but all over the world, the trend is to neglect such type of cyber crimes. They are not ready to lodge the immediate report of such cyber crimes to proper authorities. In many cases, the victims and accused persons are very well acquainted with each other, this is also one of the reasons of not complaining of such crimes.

Prevention of Cyber Crime: Prevention is always better than cure. It is always better to take certain precaution while operating the net. Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. A citizen should keep in mind the following things:

1. To prevent cyber stalking, avoid disclosing any information pertaining to one self. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and up date anti virus soft-ware to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
8. Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separately protected from internal corporate network.

Conclusion: Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. It is evident that no legislation has succeeded in totally eliminating cyber crime from the world. The only possible step is to make aware of their rights and duties (to report cyber crime as collective duty towards the society) and further making the application of laws more stringent to check crime.

References:-

1. Parthasarthy Pati - Cyber Crimes (2003) P. 79.
2. Mani's "A practical approach to Cyber laws". Kamal Publishers. First Edition, 2008.
3. Dr. Amita Verma "Cyber Crimes and Laws" Central Law Publishers. First Edition, 2009.
4. Rodney D. Ryder "Guide to Cyber Laws" Wadhwa Publications. Second Edition, 2003.
5. Various websites related with the issue.

****