Cyber-Crimes Against Women in India: Legal Perspective

Dr. Pooja
Assistant Professor
advocatepoojarao@gmail.com
Phone: +91-9899873049

Abstract

As we know crime against women is on a rise in all fields. Every second, one woman in India becomes a victim of cybercrimes and now the new platform is the online space where a woman's dignity, privacy and security are increasingly being challenged every moment. Trolling, abusing, threatening, stalking, voyeurism, body-shaming, defaming, surveillance, revenge porn and other forms of indecent representation of women are rampant in the cyber world. In cybercrimes against women, the effect is more mental than physical while the focus of the present laws ensuring women's security is more on physical than mental harm. It is true that the National Crime Records Bureau (NCRB) of India does not maintain any separate record of cyber-crimes against women. Technology is the resource used by some perpetrators who target to defame women by sending obscene WhatsApp messages, e-mail, and stalking women by using chat rooms, websites, and worst of all by developing pornographic videos, mostly created without their consent, spoofing e-mails, morphing of images for pornographic content by using various software available online. The present study aims to analyze various types of cybercrimes that can be inflicted upon a woman and how they adversely affect her. The study also briefly examines upon the various laws that exist to protect women in such cases such as the Information Technology Act (2000) and the Criminal Amendment Act (2013). This study suggests several remedies to counter the ever-increasing cybercrime against women in India. At the conclusion the focus is 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.

Keywords: Cybercrime, Crime Against Women, India, Women, Cyber Laws.

Introduction

The traditional Indian society places women in a very high regards, the Vedas glorified women as the mother, the creator, and one who gives life and worshipped her as a "Devi" or Goddess. The women occupied a vital role and as such her subjugation and mistreatment were looked upon as demeaning to not only the woman but towards the whole society. However, in modern times women are viewed and portrayed as sex objects, she is treated inferior to men in various societal spheres and functions; this has created a huge gender bias between the men and women where even the men think that their wrongdoings towards women cannot be penalized. Cybercrime and internet bullying works in similar manner where the wrong-doers are not afraid of any authority that can penalize. The cyber world in itself has a virtual reality where anyone can hide or even fake his identity, this gift of internet is used by the criminally minded to commit wrongful acts and then hide under the blanket provided by the internet.

Cybercrime Against Women

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, Cybercrimes and cyber bullying is of various types, some are:

Cyber Harassment: Cyber Harassment is characteristic repetitive behavior intended to disturb or up rest a person though use of internet. In the cyber world harassment including blackmailing, threatening, bullying, and even cheating is often done through e-mailing. Email harassment is very similar to harassing through letters; however, it is greatly difficult to crackdown upon the culprits of crime in cyber harassment as often people create fake identities on internet for such purposes.

Cyber Stalking: Cyber Stalking basically is behavior wherein an individual willfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes that person. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or pedophiles. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites and email. The motivation of stalkers may be considered less than four reasons, (i) sexual harassment, (ii) obsession for love, (iii) revenge and hate, (iv) ego and power trips.

Ritu Kohli Case was Indi's first case of cyber stalking, in this case Mrs. Ritu Kohli complained to police against a person, who was using her identity to chat over the Internet at the website http://www.micro.com/, mostly in 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 obscene language. The same person was also deliberately giving her phone number to other chatters encouraging them to call Ritu Kohli at odd hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on odd hours. The said call created a havoc in personal life of the complainant consequently IP addresses was traced and police investigated the entire matter and ultimately arrested the offender. A case was registered under the section 509, of IPC and thereafter he was released on bail.

Cyber Pornography: It refers to portrayal of sexual material on the web. This is another threat to the female citizens as they never know which actions of theirs are being recorded and would later end up on internet. The DPS MMS scandal is a very famous case of this where an MMS clip of a school girl in compromising situation was made and distributed amongst various internet networks. In another incident, at Mumbai, a Swiss couple gathered slum children and then forced them to appear for obscene photographs, which they took and then uploaded those photographs to websites specially designed for pedophiles. The Mumbai police arrested the couples for pornography. The most recent example is of Delhi Metro CCTV footage leaks case, where the CCTV recording couples getting intimate in metro stations etc. which has been recorded by police security cameras has been leaked on internet.

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. The very first instance of cyber defamation in India was recorded in the case of SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra-Jogesh Kwatra - cyber defamation was reported when a company"s employee (defendant) started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the plaintiff company. The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs. Another famous case involving women was The State of Tamil Nadu Vs Suhas Katti -The case is related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by

him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Morphing: Often criminally minded elements of the cyber world download pictures of girls from websites such as Facebook and then morph it with another picture in compromising situation so as to represent that those women were indulging in such acts. This is to blackmail those women through the threat of releasing the morphed images and diminishing the status of those women in society. Air Force Balbharati School case (Delhi) 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.

Email Spoofing: E-mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source; ill-intentioned users can make the email appear to be from someone other than the actual sender. This method is often used by cyber criminals to extract personal information and private images from unsuspecting women, these images etc. The most popular case of cyber spoofing is Gujrat Ambuja's Executive Case, in this case the perpetrator pretended to be a girl for cheating and blackmailing the Abu dhabi based NRI.

Cyber Law under the Information and Technology Act, 2000

- **Section 67** deals with publishing or transmitting obscene material in electronic form.
- **Section 66A**: Sending offensive messages through communication service, causing annoyance etc., through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such

messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine.

- **Section 66B**: Dishonestly receiving stolen computer resource or communication device with punishment up to three years or one lakh rupees as fine or both.
- **Section 66C**: Electronic signature or other identity theft like using others' password or electronic signature etc.
- **Section 66D**: Cheating by person on using computer resource or a communication device shall be punished with imprisonment of either description for a term which extends to three years and shall also be liable to fine which may extend to one lakh rupee.
- **Section 66E**: Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.
- **Section 66F**: Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization.
- **Section 72**: Punishment for breaching privacy and confidentiality.
- **Section 72A**: Punishment for disclosing information during lawful contract.
- **Section 441 IPC**: This section deals with criminal trespassing.
- **Section 354D**: This section deals with stalking. It defines stalker as a man who follows a woman and tries to contact such woman, monitors every activity undertaken by the woman while using digital media.

Protection from Getting Victimized to Cybercrimes

- Don't share passwords. You may have shared your password with a trusted

friend or partner. While friends may not intentionally cause you harm, they may accidentally reveal your password to someone. Use your discretion and keep those passwords private and complicated.

- Don't leave your webcam connected. There are too many apps capable of turning on your camera and slyly recording your movements without your knowledge. As a precaution disable camera permission and keep the lens of your camera closed or covered when not in use.
- Don't share more than necessary. Use caution when you share intimate messages, pictures, information or anything that has the potential to come back and embarrass you.
- Don't meet online acquaintances alone. Always let your friends and family know where you are going and who you are meeting. Make sure you meet the person in a crowded coffee shop or mall.
- Be careful about posting details about your whereabouts and lifestyle. Stalkers can find ways to reach you with a simple photograph or status update.
- Update all operating systems on your devices. Security updates and patches keep the latest threats away.
- Secure your devices with anti-virus software. Read the fine print Know and understand the privacy policy and terms of service of any service you use.
- Block people you don't want to interact with.

Reporting a Cyber Crime

The procedure for reporting cybercrimes is more or less the same as for reporting any other kind of offence. The local police stations can be approached for filing complaints just as the cybercrime cells specially designated with the jurisdiction to register complaint. In addition, provisions have now been made for filing of 'E-FIR' in most of the states. If a police station refuses to register the complaint, a representation may be given to the commissioner of police/superintendent of police. If in spite of that action is not taken, the next step could either be a private complaint before the concerned court or a writ before the high court. in such scenario, the woman who is victim, should first contact a women assistance cell or NGO (such as All India Women's Conference, Sakshi, Navjyoti, Centre for cyber victims counselling) which will assist and guide them through the process, also this will make sure that police does not take any case lightly.

Conclusion

The chief problem of cybercrime lies in the modus operandi and the persistence of the cybercriminal. The police, judiciary and the investigative agencies need to stay abreast with the latest developments in web-based applications so that they can quickly identify the actual perpetrator. It is the job of the legal system and regulatory agencies to keep pace with the Technological developments and ensure that newer technologies do not become tools of exploitation and harassment. Governments can take legislative measures that ensure human rights; especially women's rights are protected online just as they are physical spaces. Legislation should not just protect users; however, it should also educate and inform all groups on how to exercise their communication rights. At the same time, Individuals must become savvy both online and offline; know how to take precautionary measures in cyberspace and how to seek recourse if their rights are violated. People need to recognize the rights of others and realize what constitutes a crime. They 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 minds 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.

References

1. http://cyberlaws.net/cyberindia/2CYBE R27.htm
2. http://en.wikipedia.org/wiki/DPS_MMS _Scandal
3. G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007)
4. http://zeenews.india.com/news/nation/p orn-mmses-from-delhi-metro-cctv-footage_860933.html
5. http://cyberlaws.net/cyberindia/defamati on.htm
6. http://www.naavi.org/cl_editorial_04/su has_katti_case.htm
7. http://www.indiaforensic.com/cyberexto rtion.htm
8. http://www.aiwc.org.in/ (Private group of women assisting other less fortunate women to fight the crimes committed against them)
9. http://www.sakshingo.org/ (NGO assists women in dealing with govt authorities)
10. http://www.navjyoti.org.in/ (NGO by Kiran Bedi, assist women in several aspects)
11. http://www.cybervictims.org