VOL.5 ISSUE 1
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

CYBER CRIMES AND WOMEN

Adv. Priya Jagadeesh[1]

Abstract

In the ancient times, the women held a respective position in the society. But later on due to changes in society, women lost their status. Crime against women in India is one of the oldest customs which is still running and which became a bane of India's development efforts. As per the reports of National Crime Records Bureau, the crime against women is increasing.

In the recent decade, people explored the use internet to such an extent where the people sitting a thousand miles away can remain connected through the internet. India stepped toward digitalization which brought technological power. Hence at one side of the coin, the digitalisation has enhanced the system of India in all terms such as economy, education, governance etc. but at the same time it has opened doors too cyber criminals also.

Cybercrime is defined as an offence that is committed against individuals with malice to harm the reputation of the victim or cause physical, emotional or mental harm with the aid of modern technology. Women especially inexperienced young girls who fail to understand the vices of internet are most susceptible to falling into the bait of cyber criminals & bullies. Recently during lockdown there has been a significant increase in cybercrimes against women.

This chapter discusses about various cybercrimes committed against women and the reasons that can be attributed for its growth. Further the chapter discusses about the Indian laws dealing with cybercrimes and preventative initiatives that can be adopted to restrict cybercrimes.

[1] Assistant Professor in Law,SCMS Cochin School of Business, Kalamassery.

Introduction

India has been a patriarchal society since the time immemorial. The biological difference between men and women has named itself as dominion and women have always been considered as a commodity. Many evil customs, traditions and practices stepped in the society which enslaved the women and confined them within the boundaries of the house. In scriptures, the women's status was so high but practically it was low because women were prohibited to take part in making decisions in internal matters and as well as external matters, even in the matters of her own life like marriages. Later on, the discrimination was also observed against women in society in terms of acquisition of education and other rights and facilities.

Crime against women means direct or indirect physical or mental cruelty to women or crimes in which women are victims. The official reports clearly showed a declining sex-ratio between men and women, health status of women, literacy rate of women, work participation rate and political participation of women. While on the other hand the spread of social evils like dowry deaths, child marriage, domestic violence, rape, sexual harassment, exploitation of women workers is increasing day by day in different parts of India.

Communication has always been the most significant invention by human beings. In the recent decade, people explored using of internet and remain connected through the internet. At one side, the digitalisation helped India in all terms such as economy, education, governance etc. but at the same time it has also provided wide range of opportunities to cyber criminals. Women who fail to understand the vices of internet are most vulnerable to falling into the bait of cyber criminals & bullies.

Cybercrime and Cyber Law

Cybercrime is defined as any illegal activity in which a computer is the main object of the crime or is used as a tool to commit an offence. In its widest sense, it is an offence committed against individuals or groups of individuals with intention to harm the reputation of the victim or to cause physical, emotional or mental harm to the victim directly or indirectly with the help of modern technology and communication networks. Some examples of cybercrimes are identity theft, phishing, distribution of child pornography etc.

Women, especially young girls who are ignorant about the world of internet and new to many technological aspects like internet safety, tend to fall prey to cyber criminals. They are not aware of the problems and evils that the internet brings with its use. In fact, cyber bullies and criminals target women for crimes like virtual stalking and distribution of child pornography. Cyber perpetrators misuse the cyber platform to harass women for voyeuristic pleasure.

Cyber Law in our country is not a separate legal framework. Whereas it is a combination of contract law, intellectual property law, data protection and privacy law. While in the recent times, computer and internet are taking over almost each and every aspect of our life, hence there is a need for a strong cyber law exclusively dealing with all the crimes that are committed in the cyber with the help of technology.

Cybercrimes against women and the relating laws

Cybercrimes are proliferating at higher rate in India. Digital India have become a soft target for criminals as country recorded a huge increase of 63.5 percent in cybercrime cases in the year 2019, showed the National Crime Record Bureau data. There is no separate data available with National Crime Record Bureau data regarding the cybercrimes against women.

Most common types of cybercrimes committed against women are discussed below:

1. Cyber stalking

This is one of the most talked about internet crimes in the modern world. Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites and email. The motivation of stalkers can be attributed due to the following reasons:

a) sexual harassment,

b) obsession for love,

c) revenge and hate

The anonymity of online interaction reduces the chance of identification and makes cyber stalking more common than physical stalking. Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the Information Technology Act where the perpetrator can be booked remotely for breach of confidentiality and privacy. The accused can also be booked under Section 441 of the Indian Penal Code.

Ritu Kohli Case[2]was India's first case of cyber stalking. In this case, Mrs. Ritu Kohli complained to police against a person, who was using her name and address to chat over the Internet at the website http://www.micro.com/ 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 add hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on add hours. The said call created a havoc in her personal life. Consequently, IP

[2] Manish Kathuria v. Ritu Kohli, C.C.No. 14616/2014

addresses was traced and police investigated the entire matter and ultimately arrested the offender under the section 509 of Indian Penal Code.

2. Defamation

In this type of crime, defamatory information about a person is published on a website or circulated among the circle of the victim.

Defamation through cyber space is dealt under Section 500 of the Indian Penal Code. The very first instance of cyber defamation in India was reported in the case of *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra-Jogesh Kwatra*.[3]. In this case, a company's employee started sending derogatory, defamatory and obscene e-mails about the 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 company. The company was able to identify the perpetrator 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.

3. Morphing

This is an activity to edit original picture for the purpose of misappropriation. In this type of crime, perpetrators download pictures of women from social media life Facebook, WhatsApp or other sources and then morph it with another picture in compromising situation so as to represent that those women were indulging in such acts. Often the next step after this is to blackmail those women through the threat of releasing the morphed images and diminishing

[3] SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra-Jogesh Kwatra, Final Order dated February 12, 2014

the status of those women in society. Acts of morphing is penalised under Sections 43 & 66 of Information Technology Act and under Section 509 of the Indian Penal Code.

In *Air Force Balbharati School case*[4] 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. Proceedings were initiated in the Juvenile court, Delhi on the charge of cyber pornography. Some jurists say this is the first Indian cyber pornographic case which was charge sheeted in the juvenile court.

4. Cyber pornography

It refers to portrayal of sexual material on the web. This is the another threat to the female netizens as they never know which actions of theirs are being recorded and would later end up on internet.

Cyber pornography can be made liable under the Indian Penal Code, 1860 and The Information Technology Act, 2000 which provides limitations and prohibitions of certain things which are obscene. It prohibits sale, distribution, publication, export, import etc. of obscene books, pamphlets, papers, writings, drawings, paintings, representations and the like except justifications like literature, art, learning, monuments, etc. and prescribes punishments. It prohibits sale of obscene objects to young persons and obscene acts and songs to annoyance of others in or near any public place and prescribes punishments. It also prohibits word, gesture or act intended to insult the modesty of a woman. Whoever publishes or transmits or causes to

[4] The Air Force bal Bharti, Delhi Cyber Pornography Case 2001

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.

In the case of *Tamil Nadu v. Suhas Katti*,[5]the accused was charged for annoying, obscene and defamatory message in the yahoo message group relating to a divorce woman. The accused at first opened a false account in the name of the victim and then sent her information through e-mails. It annoyed the victim because she had to face harrowing calls. The victim filed a complaint about the fact before police. The police traced the accused at Mumbai and arrested him immediately after few days. On the basis of the expert witness the court held that the crime is conclusively proved and the accused was convicted under Section 469, 509 India Penal Code and Section 67 of the Information Technology Act.

5. Email Spoofing

It is a fraudulent email activity in which the address of the sender and other parts of the email header are altered to appear as though the email originated from a different source. It is done by properties of the email, such as the from, Return-Path and Reply-To fields. This method is often used by cyber criminals to extract personal information and private images from unsuspecting women, these images etc. are then used to blackmail those women.

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.

6. Phishing

[5] Tamil Nadu v. Suhas Katti. CC No. 4680 of 2004

It is an attempt to gain sensitive information such as username and password of the victim.

7. Trolling

This is also known as cyber bullying or Internet-bullying. It is an anti-social act of causing personal conflict and controversy online. It is done with an intention to provoke victims into an emotional, upsetting response.

Reasons for growth of cybercrime against women

The reasons for the growth of cybercrime rate against women can be categorized into two folds namely legal and sociological.

Legal Reasons

The objective of the Information Technology Act is crystal clear from its preamble which confirms that it was enacted largely for improving e-commerce hence it covers commercial or economic crimes i.e. hacking, fraud, and breach of confidentiality etc. The majority of cybercrimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmitting obscene material in electronic form),72(breach of confidentiality) of the Act.

Cyber defamation, cyber defamation, email spoofing, cybersex, hacking and trespassing into one’s privacy is domain is very common now days but Information Technology Act is not expressly mentioning them under specific Sections or provisions. Whereas Indian Penal Code, Criminal Procedure Code and Indian Constitution gives special protection to women and children. For instance, modesty of women is protected under Section 509 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences prosecuted under Indian Penal Code. Indian constitution guarantees equal right to live, education, health, food and work to women.

Ever since the 2012, Delhi Gang Rape case (*Nirbhaya Case*)[6] there has been a huge outcry over bringing out new reforms and penal provisions so as to protect women against the crimes committed against them in the recent society. Hence in 2013, Criminal Law Amendment Ordinance was introduced with several additions to the Indian Penal Code, such as to sections 354, 354 A, 354 B, 354 C & 354 D. These newly introduced provisions address the issues of MMS scandals, pornography, morphing, defamation. The transcendental nature of Internet is one of the main reasons for the growth of cybercrime. Section 75 of the Information Technology Act deals with the offences or contravention committed outside India but it is not discussing about the jurisdiction of the crimes committed in the cyberspace specially the question of place for reporting the case arises when the crime is committed in one place affected at another place and then reported at another place.

Sociological reasons

The women are more vulnerable to the danger of cybercrimes as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Most of the cybercrimes remain unreported due to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times she considers that she herself is accountable for the crime done to her. Further the women fear that reporting the crime might make their family life difficult for them, they also question whether or not they will get the support of their family and friends and what the impression of society will be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher. Even if the women decide to report, they will not lodge any official complaint and they want these matters to be handled unofficially.

[6] Mukesh and Anrs. Vs NCT Delhi, (2017) 6 SCC 1

Techniques to prevent cybercrimes

Cybercrimes being on rise, following are certain techniques that can be adopted to ensure safety and security in the cyber space:

1. Use a full-service internet security

Full service security should be used in cyber space because it provides protection against many existing and emerging malware including viruses and also helps us to protect our private and financial information when we are online.

2. Using of strong passwords

Passwords should not be repeated on different sites, and passwords should be changed regularly. The main objective of changing password is to make them more and more complicated. It is advised to use a blend of at least 10 letters, numbers, and symbols etc. Using of a password managing application can also be a great.

3. Keeping our system up to date

It is specifically important to keep computer systems and cyber security software updated. Cybercriminals are known to frequently exploit the faults in outdated software to acquire access to system. Patching these outdated software and defects decreases the possibility to be a cybercrime victim.

4. Manage your social media settings

Personal and private data should be kept hidden and secure.

5. Keep a check and knowledge of common security infringements

Knowledge on all the recent security breaches happening should be obtained and should also be equipped to defend from those breaches.

6. Precautions should be taken to defend against identity thefts

Identity thefts happen when someone tries to act as another person in order to gain money or get entry to any place. Identity thefts can be quite harmful and could lead to huge losses and even wrongful cases. Identity thefts can happen if someone gains access to a network or when connected with a free public Wi-Fi or use a hacked vpn etc.

7. Should have the knowledge on how to react if we become a victim

In case of becoming a victim of cybercrime, crime should be reported to the cyber cell. Even if the crime looks small or there is some suspicious activity, the same should not be ignored.

Conclusion

There are lots of ways and means through which perpetrators commit cybercrimes in the web space. Though women are considered to be an easy prey by cyber criminals, it cannot be assumed that other people are safe from cybercrimes. Anyone with less knowledge of the web space and safety can fall into the trap of cyber criminals. The government has formulated many laws covering cybercrimes and constituted special investigative agencies and cyber cells in almost all of the metro cities. Regardless of this development, cybercrimes are on a rise because of the unregulated access of internet and unawareness of people regarding cyber laws.

Moreover, the cybercrimes may not be put as some technological problem. Instead, this is an approach based problem as it is not the computer systems that are damaging and threatening other people, instead it is the people themselves who are exploiting technology to commit illegal activities and create an unsafe environment. Hence, the people are those who required to be cautious enough to know about the diverse methods that cyber criminals can adopt. It is advised to have an aware and involved mind-set to detect any such scenario which could lead to a cybercrime. Hence it is vital for everyone, especially women to be up to date with these crimes and take precautions to avoid any loss. It is sensible for all to know a little about cyber laws.

To conclude, 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. The women who become victims of cybercrime are not aware about the procedure that needs to be adopted to report the same. It is very common for women to not make official complaints in these cases as such matters tend to question their respect in the society. Many women want these matters to be handled unofficially. Henceforward there is an urgent need for bringing the awareness among the women regarding safety aspects that needs to be ensured while using cyber space and further on the mechanism that can adopted if they become victim. The awareness cannot come from within a single block of society but people, government and NGOs etc. need to work together to bring forth such awareness.