Dimensions of Cybercrime Against Women in India- An Overview

Shashya Mishra

Research Scholar

Babu Banarsi Das University Lucknow

Abstract

Indian civilization is one of the oldest civilization of the world. Women in our country are been given special status. They are been treated as Goddess. But with the modernization of the society their basic right are been violated. India is growing fast in the field of information technology. People are dependent on computers for their day today activities. Year 2000 was marked as a year of revolution in the field of technology. With the massive use of computers cybercrime is also increasing. Moreover women are the major victims of cybercrime in our country. Cybercrime is a new kind of crime. There are various kinds of cybercrime like cyber stalking, morphing and cyber defamation. Females are been harassed by Emails. They face the problem of cyberbullying which is very common now a days. We have Information technology Act 2000 to curb such kind of crimes but that law in itself is not very effective until people change their mindset.

Key Words Cybercrime, Human Rights of Women, Dignity of Women, Cyber stalking, Cyber defamation, Cyber trolling

Introduction

From the ancient time women are treated as Goddess. They hold a special status in the society. Even though they are having a unique place in the society they are also one of the most vulnerable group of the society. The makers of the constitution were equally concerned about the well being of the women therefore various rights are given to them as a part of fundamental rights. The penal laws are also present for protecting the dignity of women. With the changing time the crime against women is also changing. Crime is not only limited to bodily injury now a days. In the name of freedom of speech and expression people are transmitting obscene content and tarnish the reputation of women. Cybercrime is one of the most recent kind of crime against women Cybercrime consists of illegal activity conducted on a computer. Traditional crimes may be committed while using a computer, but cybercrime consists of more specific types of crimes, such as phishing schemes and

viruses.[1] India emerged as the third most vulnerable country in terms of risk of cyber threats such as malware, spam and ransomware in 2017.[2] Cybercrime is entirely different from the traditional crimes. With the emergence of technology which is for the betterment of the society is creating more problems especially for women. We can see the cases of cyber trolling on social media, harassment from E-mails etc. as one of the aspect of cybercrime against women. India has also made a separate law for the prevention of cybercrime against women. Information Technology Act 2000[3] tries to prevent the cybercrime against women effectively.

Meaning and Origin of Cybercrime

Cybercrime in broader sence means any illegal behavior by means of, or in relation to a computer system or network including such crimes as illegal possession and offering or distributing information by means of computer system[4].,Cybercrime first started with hackers trying to break into computer networks. Some did it just for the thrill of accessing high-level security networks, but others sought to gain sensitive, classified material. Eventually, criminals started to infect computer systems with computer viruses, which led to breakdowns on personal and business computers.[5]With the advent of computers in the late 1960's ,crimes were mostly related to physical damage to computer networks and telephone networks.[6]

Computer viruses are forms of code or malware programs that can copy themselves and damage or destroy data and systems. When computer viruses are used on a large scale, like with bank, government or hospital networks, these actions may be categorized as **cyberterrorism**. Computer hackers also engage in **phishing scams**, like asking for bank account numbers, and credit card theft.[7] Hacking is a term used to describe the activity of modifying a product or procedure to alter its normal function, or to fix a problem. The term purportedly originated in the 1960s, when it was used to describe the activities of certain MIT model train enthusiasts who modified the operation of their model trains. They discovered ways to change certain functions without re-engineering the entire device. The malicious association with hacking became evident in the 1970s when early computerized phone systems became a target.[8] This innovative type of crime was a difficult issue for law enforcement, due in part to lack of legislation to aid in criminal prosecution, and a shortage of investigators skilled in the technology that was being hacked. It was clear that computer systems were open to

[1] https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html
[2]Bhargava;Yuthika, India third most vulnerable country to cyber threats(Published in The Hindu April 5,2018 Pg No 7)
[3] Known as cyber law of India
[4] . Tiwari; Garima, Understanding Laws Cyber Laws & Cyber Crimes(Lexis Nexis Publication), 2014, Pg no. 8
[5] https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html
[6] https://gethackingsecurity.wordpress.com/2012/06/25/cyber-crime-history-and-evolution/
[7] https://study.com/academy/lesson/what-is-cybercrime-definition-history-types-laws.html
[8] https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

criminal activity, and as more complex communications became available to the consumer, more opportunities for cybercrime developed.[9]

International obligatios against CyberCrime-

Cybercrime investigations invariably involve considerations of privacy under international human rights law. Human rights standards specify that laws must be sufficiently clear to give an adequate indication of the circumstances in which authorities are empowered to use an investigative measure, and that adequate and effective guarantees must exist against abuse. Countries reported the protection of privacy rights in national law, as well as a range of limits and safeguards on investigations. 10As many as 39 crimes against women were reported every hour in India, up from 21 in 2007, according to Crime in India 2016 report by National Crime Records Bureau. As many as 2.5 million crimes against women have been reported in India over the last decade. Reported cases of crime against women increased 83% from 185,312 in 2007 to 338,954 in 2016.11 India is the world's most dangerous country followed by war-torn Afghanistan and Syria for women due to the high risk of sexual violence, according to a poll of global experts.

Budapest, 23/11/2001 - The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.[12]

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[13]

At the international level, the Convention on the Cybercrime, 2003 is the first and still the only convention, which seeks to address internet, and computer related crimes by securing international cooperation among member states and harmonising national laws on cybercrimes and improving investigative techniques. It was signed in Budapest, on 23 November 2001 and came into force on 1 July 2004. The Convention has an Additional Protocol which came into force on 1 March 2006. Though the Convention is an endeavor of the European Union and most of the ratifying countries are European, many non-European countries have ratified

[9] https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

[10] Comprehensive Study on Cybercrime Draft—February 2013 https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[11] http://www.indiaspend.com/cover-story/crime-against-women-up-83-conviction-rate-hits-decadal-low-18239

[12] Convention on Cybercrime https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[13] Convention on Cybercrime https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

the same, including the USA, Canada, Japan, Australia, South Africa, even Sri Lanka etc. India is yet to ratify the Convention. Bangladesh should ratify this Convention as well because the country can engage itself with the developing state of cyber laws in international level. Ratifying this Convention will help the country to improve and harmonise the national legislations relating to cybercrimes with the international standard and will facilitate Bangladesh and its authorities to have easy access to international authorities to deal with cybercrimes effectively and confidently.[14]

Various Kinds of Cyber Crime 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.

7. Trolling and Gender Bullying

Types of cybercrime that are committed against women:–

I. **Cyber stalking** is one of the most talked about net crimes in the modern world. The Oxford dictionary defines stalking as "pursuing stealthily". 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 pedophiles. Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & Internet safety. Their main target of this is Over 75% of the victims who are female.

[14] LAW VISION *URGE TO RATIFY THE CONVENTION ON CYBERCRIME* *https://www.thedailystar.net/law-our-rights/law-vision/urge-ratify-the-convention-cybercrime-1382548*

. II**. Harassment through e-mails** 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 The motives behind cyber stalking have been divided in to four reasons, namely, for sexual harassment, for obsession for love, for revenge and hate and for ego and power trips. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites (e.g. blogs and Indy media) and email. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment.

III **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 [Childnet International]. 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. "Globally, India is third behind China and Singapore in cyber bullying or called online bullying [Simhan]. Cases of suicides linked to cyber bullying have grown over the past decade.

IV **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 re-posted/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.

V 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.

VI 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

VII Trolling and Gender Bullying- The two most under- researched issues in the arena of cybercrime against women in India are gender bullying and trolling[15].On the internet women are targeted are targeted by bullies as much as young teenagers are targeted by bullies.[16] Compared to cyber bullying is a new phenomenon in India.Trolls basically diverts the focus of publication. The troll posts are essentially provocative posting intended to produce a large volume of frivolous responses.[17]

Crime against Dignity of Women-

Article 19(1)(a) of the constitution provides fundamental right to speech and expression. This right is not absolute and is subject to reasonable restrictions that are mentioned under Article 19(2).

The Information Technology Act 2000 after its amendment in 2008 has provided for such reasonable restrictions. These are in the form of powers granted to central or state Governments to issue directions for interception, monitoring or decryption of any information through any computer source located in India.[18]

Offensive speech against women-

The advent of the internet has expanded the reach of freedom of expression for millions of internet users. Information wants to be free and the internet fosters speech and expression for providing basic right. In Neelam Mahajan Singh V. Commissioner off Police on the question of the balance between freedom of speech and expression and public decency it was held: ―We need not to attempt to bowdlerize all literate and thus rob speech and expression. A balance should be maintained between freedom of speech and expression and public decency and morality but when the latters is substantially transgressed the former must give way:

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. [Mukut 2012]. Stalker used obscene and obnoxious language, and post 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

[15] Halder Debarati, Jaishanker,H; Cyber Crimes Against Women In India,pg. no. 43
[16] ibid
[17] Ibid pg 62
[18] Duggal;Pawan, Textbook on Cyber Law, Pg.no 13

complaint. Fortunately Delhi police immediately sprang into action. They traced 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 [Mukut 2012]

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

Infringement of right to Privacy-

The display of information in cyber world has a close nexus to right to privacy

Now a days internet has become a vital communication medium and people use their freedom of speech and expression guaranteed under the Indian Constitution. But this freedom is not absolute therefore changes are done in the IT Act also.

In Shreya Singhal vs Union of India (2015) the Court struck down Section 66A of the IT Act in its entirety holding that it was not saved by Article 19(2) of the Constitution on account of the expressions used in the section, such as “annoying,” “grossly offensive,” “menacing,”, “causing annoyance. Apart from not falling within any of the categories for which speech may be restricted, S66A was struck down on the grounds of vagueness, over-breadth and chilling effect

Penal Provision on Cybercrime Against Women in India

The Indian Penal Code provides for various offences against women.

(i) Obscenity- Provision relating to obscenity have been included in section 292-294 of the Indian Penal Code, 1980. They deal with sale, hire, distribution, public exhibition, circulation, import, export or advertisement etc. of many matter which is obscene. Section 292 and 293 IPC were amended in 1969 to mate the existing laws more definite in Explaining the term obscenity. In order to make the law relating to publication of obscene matters deterrent, the section provided enhance punishment. According to Section 292 of Indian Penal Code.74 [(a) For the purpose of sub-section (2) book, Pamphlet, Writing, Drawing, painting, representation, figure or

any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if it effect, or (where it comprises two or more distinct items the effect of any one of its item is if taken as a whole, such as to tend to deprave and corrupt person who are likely, having regard to all relevant circumstances, to read, are or hear the matter contained or embodied in it.

whoever sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes produces or has in possession any obscene book, pamphlet, paper, drawing, painting representation or figure or any other obscene object, whatsoever or (b) Imports, exports or convey any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicity exhibited or in any manner put into circulation or. (c) Take part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the Sub-section (2) of that section purpose aforesaid, made, produced, purchased kept imported, exported, conveyed, publicly exhibited or in any manner put into circulation. (d) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section or that any such obscene object can be procured from or through any person

Sec 293 of the Indian Penal Code provides for Sale, etc of obscene objects to young person-

Section 294 of the Indian Penal Code makes provision for obscene acts and songs. This section reads as follows: ―Whosoever to annoyance of others, (a) does any obscene act in any public place, or (b) sings, recites or utters any obscene songs, ballad or words, in or near any public place. Shall be punished with imprisonment of either description for a term which may extend to three months or with fine or with both.

Insult to Modesty-

Section 509 of the Indian Penal Code applies to all women. Law

Outraging the Modesty

Section 354 of the Indian Penal Code provides for outraging the modesty According to this section ―whoever assaults or uses criminal force on any women, intending to outrage or knowing it to be likely that he will thereby, outrage her modesty, shall be punished with imprisonment or either description for a term which may extend to two years, or with fine, or with both.

Information Technology Act 2000

This act is known as the cyber law of India. It is India's mother legislation, regulating the use of computers, computer system, computer networks, communication devices as also data and information in electronic format. This legislation has touched various aspect of crime like cybercrimes and liability of network providers. The said act was amended in the year 2008Due to amendment all kinds of cell phones, phones, tablets and personal digital have been brought within the ambit of cyber law.

Salient Features of the Act related to cybercrime against women-

Information Technology Act 2001 is a key weapon to prevent cybercrime. The act basically deals with online transaction but some its provisions deals with the offence against human body. The major provisions of the Act are as follows-

Electronic obscene content-

Section 67 of IT Act prevents publishing and transmitting of obscene contents on the internet which disturbs public order and morality. It is based on sec 292 of IPC. But the amount of punishment is higher in IT Act2000. It is a bailable offence.

Sending of offensive messages

Section 66 A provides for the offence of sending offensive messages through communication devices or computer resources. Section 66A makes it a offence when it is send by means of a computer resource-

- Any information that is grossly offensive
- Any information that has menacing character
- Any information which you know to be false but which is sent for the purpose of causing insult

Spam Messages

It is important that 66A©tries to cover slightly the phenomenon of spam.But this provision is not very effective.

Identity Threat-

Section 66 C has provided for the offence of identity theft. The said offence is bailable offence where the accused even if arrested be entitled to bail as a matter of right.

Cheating by Personation by computer resources

If the person cheats by pretending to be another person who is already predeceased by using computer system, computer networks and computer resources or communication devices, he is deemed to have committed the offence of cheating under section 66 D

Violation of Privacy-

Another Section 66E has been added to provide for the offence of violation of privacy.

Following essential acts need to be performed-

1-Capturing

2-Publishing

3-Transmtting

Transmit means to electronically sending visual image.

National Cyber Security Policy 2013 For preventing Cybercrimes-[19]

India now has a policy which provides for the legal basis for the cause of cyber security in India. It has 14 objectives to create cyber- ecosystem in India. One of the key objectives is to facilitate monitoring at national level such as cyber security compliance, cyber attacks, cyber- crime and cyber infrastructure growth.

Suggestion and conclusion

The cybercrime against women is increasing at a very fast rate new offences like trolling and gender bullying are emerging as new field of cybercrime. But the IT Act 2000 does not include such crimes and the process of investigation is not appropriate. Act do not provide any remedy to cyber tolling and gender bullying which is one of the lacunae of the act.There is a need to create separate cell for the investigation. Special training must be given be the officers to deal with the cybercrimes against women. Judicial system of the country should try to tackle the problem of cybercrimes against women effectively.

[19] Tiwari; Garima, Understanding Laws Cyber Laws & Cyber Crimes(Lexis Nexis Publication) 2014