Quest Journals
Journal of Research in Humanities and Social Science
Volume 8 ~ Issue 1 (2020) pp: 75-79
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Cyber Crime Against Women in Indian Context: An Overview

Priya Gupta
Research Scholar, Department of Law, Deen Dayal Upadhyaya Gorakhpur University,Gorakhpur

Abstract:
Indian civilization is one of the oldest civilizations of the world. From the ancient time women were treated as Goddess in India. They hold a special status in the society. But there has been an increase in crime against women in India since the time of external invaders, be it ancient times or modern times, crimes against women have been happening only now the form and platform of crime has changed, which crimes against women used to be in the physical world, Crimes are now happening in Cyber World like eve teasing, bulling, abusing, modesty, harassment, black mailing.Cyber crime in India in the age of information technology which basically happen to Indian women is Cyber Space such as harassment through e-mail, cyber-stalking, cyber defamation, morphing, email spoofing, hacking, cyber pornography, cybersex trafficking, cyber sexual defamation, cyber eve teasing. But at present in India, the existing laws are not fully capable to deal with cyber crime, there is a need to make these laws more efficient and strict.

Key Words: *Cyber Crimes, Cyber crime against women, Human Rights of Women, Cyber stalking, Cyber defamation, Cyber trolling, Cyber pornography, Cyber bullying, Cyber grooming, Cyber phishing.*

I. Introduction:

Crime against women have increased rapidly in the last few years. From ancient times to the present time also there are some crimes which are happening against women like eve teasing, bullying, abusing, modesty, harassment but in the present time, the way of committing these crimes and their platform has changed, which we get to see in cyber space as cyber crime.

Meaning:
Cyber crime in a broader sense 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.

Historical Background of Cyber Crime In World:
While cyber crime existed before this, the first major wave of cyber crime came with the proliferation of email during the late 80"s. It allowed for a host of scams and/or malware to be delivered to your inbox. The next wave in the cyber crime history timeline came in the 90"s with the advancement of web browsers. At the time there were a multitude to choose from, many more than today, and most were vulnerable to viruses. Viruses were delivered through Internet connections whenever questionable websites were visited. Some caused your computer to run slow; others may have caused annoying pop-up advertising to crowd your screen or redirect you to the nastiest porn sites. Cyber crime really began to take off in the early 2,000"s when social media came to life. The surge of people putting all the information they could into a profile database created a flood of personal information and the rise of ID theft. Thieves used the information in a number of ways including accessing bank accounts, setting up credit cards or other financial fraud. The latest wave is the establishment of a global criminal industry totaling nearly a half-trillion dollars annually. These criminals operate in gangs, use well established methods and target anything and everyone with a presence on the web.

International Concern for Cyber Crime:
In order to protect women from Cyber Crime various international conventions, conferences, treaties, international agreements, international institutions and various countries have contributed by cooperating at the international level. For example, Budapest is the first convention to provide protection from Cyber Crime, some international organizations that cooperated are Asia-Pacific Economic Cooperation, Professional efforts of International Criminal Police Organization (Interpol), United Nations and European union and some countries have tried to eliminate Cyber Crime by including Cyber Crime law in their national law, which are USA,

Canada, Japan, Australia, South Africa, Sri Lanka, India, Bangladesh

Historical Background of Cyber Crime Against Women In India:

Indian civilization is one of the oldest civilizations of the world. From the ancient time women were treated as Goddess in India. 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 groups of the

society. But there has been an increase in crime against women in India since the time of external invaders, be it ancient times or modern times, crimes against women have been happening only now the form and platform of crime has changed, which crimes against women used to be in the physical world, Crimes are now happening in Cyber World like eve teasing, bulling, abusing, modesty, harassment, black mailing. Cyber crime in India in the age of information technology which basically happen to Indian women and is Cyber Space such as harassment through e-mail, cyber-stalking, cyber defamation, morphing, email spoofing, hacking, cyber pornography, cybersex trafficking, cyber sexual defamation, cyber eve teasing. The computer era in India had started from 1953, but before the passage of the Information and Technology Act 2000, the punishment for Cyber Crime was given under the Indian Penal Code 1860. But Indian Penal Code was not fully competent to make provision of punishment in respect of Cyber Crimes, so to prevent cyber crime, Information Technology Act, 2000 was passed in the year 2000. In 2008, provision of punishment was made in the Information Technology Act, 2002 by including new Cyber Crimes. In view of the changing nature of Cyber Crime at present, there is still a need to make changes in Information Technology Act, 2000. This act is still not able to provide full punishment for Cyber Crime against women. At present, Cyber Cell in India is also working to remove Cyber Crime and efforts have been made to remove Cyber Crime by amending the National Cyber Security Policy from time to time. Girl child victims of can now lodge their complaints at National Commission for Protection of Child Rights (NCPCR)'s POCSO e-box. POCSO e-box is an easy and direct medium for reporting of girl child sexual abuse under the Protection of Children from Sexual Offences (POCSO) Act, 2012[1]. Similarly, the POCSO Act is also not fully capable of preventing cyber crime against girl child like the InformationTechnology Act, 2000 and Indian Penal Code, 1860.

Some Major Cyber Crime Against Women in India:

Major Cyber crimes are as under:

- **Cyber Bullying**: A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc. sexual act.
- **Cyber Stalking:** Cyber stalking is on the rise and women are the most likely targets. Cyber stalking is a way to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threat to a victim but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation.
- **Harassment through e-mails**: 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-Harassment is similar to the letter harassment but creates problem quite often when posted from fake ids
- **Cyber Defamation**: Cyber defamation includes both libel and defamation. It involves publishing defamatory information about the person on a website or circulating it among the social and friends circle of victims or organisation which is an easy method to ruin a women's reputation by causing her grievous mental agony and pain.
- **E- Mail Spoofing**: it generally refers to an e-mail that emerges from one source but has been sent from another source. It can cause monetary damage.
- **Cyber Phishing**: Phishing is the attempt to gain sensitive information such as username and password and intent to gain personal information.
- **Cyber Morphing**: Morphing 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 websites by cresting fake profiles after editing it.
- **Cyber Trolling**: Trolls spreads conflict on the Internet, criminal's starts quarrelling or upsetting victim by posting inflammatory or off-topic messages in an online community withthe intention to provoke victims into an emotional, upsetting response. Trolls are professional abusers who, by creating and using fake ids on social media, create a cold war atmosphere in the cyber space and are not even easy to trace.

- **Cyber Grooming**: Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.
- **Cyber Pornography**: Cyber Pornography is the other threat to the female netizens. This would include pornographic websites; pornographic magazines produced using computers and the internet.
- **Cybersex Trafficking:** Unlike sex trafficking, the victim does not come in direct contact with the abuser. In cybersex trafficking, the dealer live-streams, films, or photos of the victim performing sexual/intimate acts from a central location and sells the material online to sexual predators and buyers. The offenders have been sexually abusing children by making them a part of cybersex trafficking byways of manipulation and coercion.

Legal Provisions:

The Constitution of India, 1950: Article 19 and 21 provides protection to women from Cyber crime. 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). And Article 21 of the constitution gives right to women in India to live in cyber space with human dignity.
Indian Penal Code, 1860: Penal provision on Cyber crime against women in India under Indian Penal Code the Sections are- Section- 292-294 for *O*bscenity, Section 509 For Insult to Modesty, Section 354 for Outraging the Modesty (Section 354A-354D), Section 292,293,294,504,509 for Pornography. And Section 379,405,420 for Data Theft.
Information Technology Act:
Under IT Act, 2000 Sections are 66A for Sending offensive messages through communication service, Section 65 for Tampering with computer source documents, Section 70 for Tampering of confidential information, Section 72 for Online stalking, Section 42A and Section 66 of IT Act, 2000(r/w Section 379,406 of IPC, 1860) for Data hacking, Section 43B,66E and 67C for Data Theft, Section 67A for Pornography.

The Copy Right Act, 1957:
Section 63B of Copy Right Act, 1957 provides protection to women from Data Theft. This section provides that any person who knowingly makes use of a computer or an infringing copy of a computer program shall be punishable.

Protection of Children from Sexual Offences (POCSO) Act, 2012:
POCSO Act, 2012 provides protection to girl child, the provisions are- Section 3 for Penetrative Sexual Assault, Section 5 for Aggravated Penetrative Sexual Assault, Section 7for Sexual Assault, Section 9 for Aggravated Sexual Assault, Section 11 for Sexual Harassment of the Child, Section 13 for Use of Child for Pornographic Purposes.
The constitution of India guarantees equal right to life, right to live with human dignity andright to speech and expression to women but the same modesty of women seems not to be protected in general in the Information Technology Act, 2000. There are no specific provisions in the IT Act, 2000 that specifically deal with the crime against women as do theprovisions of the Indian Penal Code, the Constitution of India or the Code of Criminal Procedure for that matter. Similarly, the POCSO, 2012 is also not fully capable of preventing cyber crimes against gild child like the Information Technology Act, 2000 and Indian Penal Code, 1860.

Judicial Decisions:
A leading case of supreme court ***Ranjeet. D. Udeshi vs. Maharashtra*** is the first major case to explain cyber obscenity in India.
There was a Court recorder in London during the era of the 19th Century. His name was Benjamin Franklin and after his name the test was named as "Hicklin Test". Basically, it is an obscenity standard that originated in an English case- ***Regina vs. Hicklin (1868)***, this case is based on women pornography and obscenity, in this case a propounded doctrine named Hicklintest is a standard of obscenity in context of women pornography.

In *2002*, ***State of Tamilnadu vs. Dr. L. Prakash***' this case is the this first in India to punish in relation to offence of transmitting obscene material in electrical form under section 67 of Information Technology Act 2000.
Manish Kathuria vs. Ritu Kohli[2]this case is the first case in India dealing with cyber stalking, in 2001 first time cyber stalking's case had been reported in India. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police

registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended

to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under thesame. So, in 2008. Indian legislature has amended the IT Act 2000 and made provisions for cyber stalking. The IT Act, 2008 does not directly address stalking. But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in the IT Act, 2008. Hence the most used provision for regulating cyber stalking in India is Section 72 of the IT Act, 2008

An Important case of Supreme court ***Shreya Singhal vs. Union of India****' this* case is one of the latest cases on protection of cyber crime against women on social media which is a threat to women in cyberspace, protecting freedom of expression, in this case, S.66A of the Information Technology Act 2000 (inserted vide amendment in 2008) was struck down by the Supreme Court as unconstitutional. The court took this historic decision after the petition alleged that the said provision is extremely vague and it is being misused grossly for curtailing freedom of speech in cyberspace in India. But while it is accepted that the provision may be a draconian law, could the Supreme court use this opportunity to re-frame and reproduce the provision for regulating certain types of speech which may be termed as „bad talk" in the internet? It may be noted that in India cyber bullying and trolling, online gender harassment, smashing and vishing are becoming rampant. The court could have considered the Therapeutic Jurisprudential value ofS.66A to recreate a better law.
In 2004 ***State of Tamil Nadu vs. Suhas Kutti,*** it was the first conviction case under the Information technology Act, 2000. Indian court firstly convicted for the offence of cybercrime.The judgment was pronounced in the year 2004, within the seven months after filling the FIR, which brings the conviction for the cybercrime.

Some Landmark cases of supreme court are, ***Papers Ltd. & others vs. Union of India****' RomeshThappar vs. The State of Madras*' that accepted level freedom belonging speech lying democracy foundation; ***Bennett Coleman & Co.& Others vs Union of India& others,*** that spoke regarding public censure basement of democracy; ***S. Khushboo vs. Kanniamal & Others,*** that spoke recording freedom significance belonging expression, speech also showcase towards tolerance in regards not so popular opinions and not so on.
National Cyber Security Policy 2013 For Preventing Cyber Crime:

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 isto facilitate
monitoring at national level such as cyber security compliance, cyber attacks, cyber- crime and cyber infrastructure growth.

II. Conclusion and Suggestions:

In the Indian scenario, the cases of cyber crime against women are increasing rapidly, in which some of the new crimes are cyber trolling and cyber bullying. 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. Similarly, cyber stalking is also a serious crime, to deal with which there is a need to make strict laws by amending the IT Act, 2000. And the majority of cyber crime need to be made non- bailable offences. There is a need to create separate cell for the investigation. And a separate law needs to be made. A comprehensive data protection regime needs to be incorporated in the law to make it more effective. Special training must be given be the officers to deal with the cyber crime against women. And the judiciary of India will have to make an important contribution to stop the cyber crime against women happening in India. The Indian government should work towards bilateral cooperation with other countries for exchanging of information on cyber crime.

References :

[1]. https://www.google.com/amp/s/www.vskills.in/certification/tutorial/cyber-crimes-2/%3famp
[2]. https://www.le-vpn.com/history-cyber-crime-origin-evolution/
[3]. https://i-probono.com/case-study/cybercrimes-against-children/
[4]. https://vikaspedia.in/social-welfare/women-and-child-development/ womenhttps:// vikaspedia.in/socialwelfare/women-and-child-development/women-development- 1/legalawareness-
[5]. https://blog.ipleaders.in/cybercrime-women-children-escalation-cybercrime- Pandemic-laws-curb/
[6]. https://vikaspedia.in/social-welfare/women-and-child-development/ women
[7]. https://blog.ipleaders.in/cybercrime-women-children-escalation-cybercrime- pandemichttps://blog.ipleaders.in/ cybercrime-women-children-escalation- cybercrime- pandemichttps://blog.ipleaders.in/cybercrime-women-children- escalation-cybercrime-

pandemiclawscurb/laws-curb/laws-curb/
[8]. The Constitution of India, 1950
[9]. Indian Penal Code, 1860
[10]. Information Technology Act
[11]. POCSO Act, 2012
[12]. The Copy Right Act, 1957
[13]. LR 3 QB 360
[14]. https://www.itlaw.in/dr-l-prakash-vs-state-of-tamil-nadu-2002 /
[15]. https://dullbonline.wordpress.com/2020/10/14/ritu-kohli-case /
[16]. Writ petition (criminal) no.167 of 2012
[17]. outlawing cyber crimes against women in India https://docs.manupatra.in› articles› upload
[18]. Dr. Jai Narayan Pandey, Indian Constitution, Central Law Agency, Forty-Three Edition, 2010.