Cyber Crime: A Women's Nightmare

Yashprada Joglekar
Adv. 29, Recreation Ground, Choubey Colony Raipur Chhattisgarh,492001, India

Abstract

Much to its disguise, Cyber-crime has now become a global phenomenon. With the emergence of new updates in technologies and innovations has made women the one of the most vulnerable victim of cyber-crime. There has been a considerable rise in violence against women in the present era and the reasons are being wide spread. Cyber-crime is considered as one of the most volatile reason for increase in violence against women. The authors in this paper will be discussing in details about how cyber-crime have let to increase in violence against women. The authors have divided the paper into six different parts. Part I will have a brief description on violence against women. In part II, authors have defined cyber-crime and have shown how women's are victimized by it. The part III will be discussing the various ways by which the technologically intellectual people i.e. hackers/cyber-criminal from around the world converts cyber world into nightmare for most of the internet user(especially women) through Cyber-stalking, Cyber-pornography, Defamation, Morphing, Harassment through e-mails, E-mail spoofing. In part IV, keeping in mind the era of social networking the authors will also be discussing in details one of the most social yet unsocial means used against women i.e. Social Engineering. The paper in part V the authors with their understanding of the Indian law will be discussing provisions for cyber-crime against women in India, the loopholes in it and latest amendments in the Indian Penal Code. Last but not the least, in part VI; will discuss the cyber-crime affecting women in Indian prospective and its growth in India.

KEYWORDS: cyber, women, crime

INTRODUCTION

Violence against women is a global social problem and is manifested in many ways, such as physical, sexual, psychological abuse in the home; rape of women in interethnic conflicts (e.g., Sudan, Congo, Libya etc…); sex trafficking; genital mutilation; and now a day's virtual abuse over the internet i.e. cyber-crime which has also different forms of abuse like cyber-stalking, cyber pornography etc. . These acts are not random; male perspectives are overrepresented, and girls and women are disproportionately the victims. Although particulars incidents are headline grabbing, the reality is that violent acts against women and girls are committed every day. Further these types of violence are situated in institutional arrangements of power and authority as well as individual factors and advancement of technology, the link being gender as an organizing instrument of social control. The need for research and policy attention to violence against women has become important internationally. As per a newspaper report, online survey was conducted in the summer of 2017 with a sample size of 1,035 respondents drawn mainly from Tier 1 cities, with the objective of understanding Indian exposure to online harassment. Threats of physical violence experienced by the respondents was highest in Mumbai (51%), followed by Delhi (47%), and Hyderabad (46%). Similarly, online sexual harrassment was reported to be highest in Delhi and Mumbai (43%), followed by Kolkata (37%) and Bengaluru (36%).[1]

CYBER- CRIME: DEFINITION

Cyber Crime is one of the most portentous of the crimes that confronts us today. Security in the cyber world is one the most sensitive issues in the gamut of cyber laws. The over exploitation of computers is also the dawn for a new age crimes that are addressed by the Information Technology Act, 2000. As the internet rapidly enters the home of the common man through computer, television, and cell phones and so on, it emerges that cyber-crime is not a threat only to dot-com and e-commerce gurus, but also the internet community at large. It is estimated that about 500 million people can be affected by cyber-crimes and the extent of losses that would be incurred is enormous.

The concept of cyber-crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which causes breach of rules of law and counterbalanced by the sanction of the state. Cyber Crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plant is being rum on computers, cyber-crime has assumed rather sinister implication. If life is about a mix of good and evil, so is the internet. For all the good it does, the cyberspace has its dark sides too. Unlike conventional communities though, there is no policemen patrolling the innocent, the information super-highway, leaving it open it everything from Trojan horses and viruses to cyber stalking, trademark counterfeiting and cyber terrorism.[2] The lack of potential jurisdiction or rather a defined jurisdiction makes it even simpler for the hacker to roam freely undetected.

Forms of Cyber-Violence against Women

With advancement of technology, cyber-crime and victimization of women are on the high and it poses as major threat to the security of women. The new cyber-crime of cyber-violence against women includes cyber-stalking, cyber pornography; email-harassment and using internet to publish obscene information to exploit or embarrass women is taking alarming proportions.[3]' There are various form of cyber-crime is committed against individual and society at large.

1. **Email as a Means of Harassment via Emails**

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[4]. Research finding strongly suggests that cyber stalkers use emails as the primary means of harassing and threatening victims, far more than any other electronic communication devices. Email allows an offender to repeatedly transmit harassing, threatening, hateful or obscene messages, including pictures, videos or audio. Cyber stalkers have known to send the victim’s private information to websites that cater specially to pornography in the hopes that the site will continuously inundate the victim with obscene email messages and pop-ups.[5]

2. Cyber- Stalking

Cyber Stalking is one of the most talked about net crimes in the modern world. Stalking defined as "pursuing stealthily" under Oxford dictionary. Cyber Stalking is fundamentally an extension of traditional stalking, in which the offender uses a hi-tech modus operandi to commit the crime.[6] This web has reached that virtual web too, with advent of cyber-stalking, which is quite common today. Cyber stalking involves following a person's movement across the cyber-space by constantly/repeatedly engaging in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes that person i.e. women victims. Stalking in the internet happens when the stalker follows the victim continuously by leaving unwanted messages through emails or by entering the chat rooms which is used by the victim.[7] Cyber Stalking usually occurs with women, who are stalked by men, or children (girls) who are stalked by adult predators. Their main targets are the mostly females, children, emotionally weak or unstable, etc. moreover it is alleged that Over 75% of the victims are female. The motives behind cyber stalking by the stalkers have been divided in to four reasons

- Sexual Harassment
- Obsession for love
- Revenge and Hate
- Ego and Power Trips.

Most of the cyber-stalking cases are reported by the women between the ages of 15-35. There are some examples of Cyber-Stalking against women which is as follows:

- In June 2000, a man was arrested by the Delhi police for assuming the identity of his ex-employer’s wife in a chat channel and encouraging others to telephone net. The victim who was getting obscene telephone calls at night from stranger made a complaint to the police. The accused was then located “on line” in the chat room under the identity of the, victim and later traced through the telephone number used by him to access the internet.
- Another case took place at New Delhi, where a man named Manish Kathuria stalking an Indian lady, Miss Ritu Kohli by illegally chatting on the Web site MIRC using her name. He used obscene and obnoxious language, and distributed her residence telephone number, inviting people to chat with her on the phone. As a result of which, Ritu kept getting obscene calls from everywhere, and people promptly talked dirty with her. In a state of shock, she called the Delhi police and reported the matter. Without wasting any further time the police department swinging into action, traced the culprit and

slammed a case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli.

3. Cyber-Pornography

Cyber-pornography is pornography that is distributed via the internet, primarily via websites, peer to peer file sharing, or Usenet newsgroups. It is a great threat to women integrity, image and character through pornography websites, pornography magazines produced using computers to design and publish the pornography material and the internet to circulate different material like porn videos, naked pictures of women etc among different male person interested in pornography. If a person found, uploading or circulating child abuse videos or pictures which are listed as serious offences under the Information Technology Act, it will immediately attract a punishment of up to 7 years and fine of Rs 10 lakh.

Now a day with advancement technology and more use of cyber-space has facilitated a medium for cyber-pornography. Now almost all the websites have pop-ups with pornography advertisements. There are few cases of cyber-pornography

- A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs 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. It was only after the father of one of the class girl features on the website objected and lodged a complaint with police that any was taken.
- Another case of IIT Kharagpur student Ravi Raj, who placed on the baazee.com a listing offering an obscene MMS video clip for sale with the username alice-elec. Despite the fact that baazee.com have a filter for posting of objectionable content. Upon investigation, a charge sheet was filed showing Ravi Raj, Avnish Bajaj, the owner of the website and Sharat Digumarti, the person responsible for handling the content, as accused. Since, Ravi Raj absconded; the petition was filed by Avnish Bajaj, seeking the quashing of the criminal proceedings.[8]

Like this there are many example of cyber-pornography against women.

4. Cyber- Defamation

Cyber tort includes libel and defamation over net i.e. cyber space is another form of cyber violence against women. It occurs with the help of computers and internet someone publishes derogatory or defamatory information to all the women's friends and people associated with her.

5. Morphing

When any unauthorized uses a fake identity to download victim's pictures, and then upload or reloads/ re-posts them on various websites especially in porn websites and sometimes even by creating a fake profile in various social networking websites, after editing the original pictures is called morphing. They also message via e-mail, with morph photographs - placing the victim's face on another, usually nude, body

6. **Revenge Porn**:

This is a form of malicious sharing of private sexual images mainly. It involves the online dissemination of private sexual images, sometimes on specially designed pornographic websites, often following a relationship break-up[9]. Holly Jacobs, whose boyfriend posted intimate images of her on a revenge porn website soon after the ordeal Holly, set up the campaign "End Revenge Porn" in America, which is part of the 'Cyber Civil Rights Initiative'. Several states in America have followed suit, Brazil, the Australian state of Victoria, and Israel. There is now a move towards the criminalization of revenge porn in England and Wales[10]. Research by CCRI has shown that 1 in 10 ex-partners threaten to post sexually intimate images online. 60% of those ex-partners end up posting those images. 90% of victims are women.[11]

7. **Email Spoofing**

Spoofing often includes attempts by crackers to create fake records or messages in a system.[12] 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 i.e. Spoofed email has misrepresented its origin. The more common method used by men is to email vulgar photographs of themselves or others or misrepresent themselves to be someone else actually to women, praising their beauty, looks and asking them for a date or inquiring how much they charge for 'services'.

.SOCIAL ENGINEERING: A BANE FOR WOMEN

Social Engineering is a non-technical way that takes advantage of native or inadequately trained employees. In other words, some cyber-crimes are committed without much sophistication. The perpetrators simply capitalize on the 'weakest links'' in the system.

Social engineering describes the deceptive process whereby crackers 'engineer' a social situation to allow them to obtain access to an otherwise closed network. Typically, the objective of this exercise is to get others- the weakest links- to reveal information that can be used to copy or steal data. For example: A cracker could talk a computer help desk employee into resetting the password on a stolen account. Once a password was obtained, access to the system by the cracker could be either permanent or temporary.

One of the most notorious social engineers in the computer underground went by the pseudonym of Susan Thunder. Susan Thunder was reportedly mistreated as a child and became prostitute in her teens. In her spare time, Susan Thunder fraternized with several rock bands. She was educated in social engineering and was known to be a *dynamic phreaker*. She gradually and eventually discovered how easy it was to get backstage passes for concert just by calling appropriate and pretending to be, for example, an executive at a record company- a form of social engineering. She was acknowledged to have the skills necessary of accessing security systems and showing the flaws in the military's computer security. She was more famous than most because of her association, and believed relationship with Kevin Mitnick. Eventually the team of three cracked into U.S. Leasing's systems, deleted all of the information of one computer, filled the computer with filthy messages and programmed the printers to continuously print out insult words. She was the main person who testified against him.

The enormous effect lack of time due to hectic work schedule, people are tending more towards social networking, as the internet rapidly enters the home of the common man, through computers, tablets, mobile phones and so on. The inhuman intellectual people from round the world socialize with women, develops a good relation with them, take them in confidence and then the real game starts of cyber-crime.

INDIAN LAWS ON CYBER-CRIME AGAINST WOMEN

In India, women's are treated as Goddess, given the highest level of respect; the women's are evidently being victim of cybercrimes and is the most traumatic experience for them.

How and why does it happen? Who does it? What are the penal laws? How to make use of these laws? These are few of the questions which arise when we deeply analyse the evil of cyber world, cybercrime.

The case from the year 2013 had been extremely disturbing: The controversial death of Dalit boy, loved and married, Divya who belong to other Hindu sub-cast and Delhi Metro Intimacy case. As well much recent case of Child pornography that broke the internet on February 22, 2018. The CBI booked Nikhil Verma from Kannauj in Uttar Pradesh; Nafees Reza and Zahid of Delhi: Satyendra Om Prakash Chauhan of Mumbai and Adarsh of Noida.[13] Besides India, Pakistan and the US, the members of the group also hailed from including China, New Zealand, Mexico, Afghanistan, Brazil, Kenya, Nigeria and Sri Lanka, the officials told. On the other side[14], case which gave country capital a jolt, Delhi Metro Sex Tape Case. On July 9, 2013 Almost all newspapers reported that CCTV footage of couple's intimacy in Delhi Metro Stations have reached the porn sites. Question arise CCTV footage of protected areas in porn sites? Government surveillance system has now brought huge embarrassment for these young couples. More so, it would obviously be the women who would be focused more than the man in the porn sites.

It is shocking to find out that many city police websites do not give proper contact details of cyber-crime cells where the victim can personally go and report the problem. E-mails and contact numbers given there are mostly non operative or non-responsive. Hence extremely reluctance to visit the police is very evident in a victim.

➢ Provisions and Laws

India has some very strict law for cyber-crime against women. The Indian Information Technology Act 2008 voices the concern.

- If someone wants to defame women online with false ‘stories’ (enough to make the victim ‘annoyed’ and the recipient ‘confused’) and sends it to huge audience cherishing the ‘gossip’, Section 66(A) of the said act will promptly sentence him/her for imprisonment which may extend to two or three years.

- If perpetrator prefers to put on filthy ‘lascivious’ words and pictures of the victim’s by doctoring the picture, Section 67 of the said act has provision of imprisonment sentence for two to three years.

- If committer wants to make the victim ‘ashamed’, ‘disguised’ or ‘traumatized’ by publishing compromising pictures where he claims to accompany his victim, no matter what, Section 67(A) can give him/her imprisonment sentence for minimum of five years and is also a non-bail able offense. The perpetrator may even be imposed with monetary fines along with imprisoning sentence.

- Section 500, section 501 and section 509 of Indian Penal Code will come to scene if the question involves defamation and ruining the modesty of the women.

- Section 292(A) of Indian Penal Code also awaits to be incorporated, if the perpetrator plans to circulate doctored pictures, pictures of intimate moments or ‘please keep secret’ stuff to blackmail his victim.

- Section 354Dof IPC is for protection of women from being stalked by men will be treated as a cognizable offence. It says, "To follow a woman and contact, or attempt to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitor the use by a woman of the internet, email or any other form of electronic communication. There are exceptions to this section which include such act being in course of preventing or detecting a crime authorized by State or in compliance of certain law or was reasonable and justified."

- **Loopholes in Indian Law**

There are certain areas in the Information Technology Act 2000 which need to be reformed in order to have a better code of law:

- Tampering with computer source document (S.65)

- Hacking with computer system (S.66)

- Publishing of information which is obscene in electronic form (S.67)

- Access to protected system (S.70)

- Breach of confidentiality and privacy (S.72)

- Publication of fraudulent purposes (S.74)

There are very fundamental problems, which are associated with Cyber-crimes are: Jurisdiction, Lack of cyber army, Lack of evidence, and cyber savvy judges who are in great need of the day. Judiciary plays a vital role in structuring the enactment according to the order of the day. One such stage, should be appreciated, is the P.I.L., which the Kerala High Court has accepted through an email once. Today with the growing hands of cyberspace and effect of globalization the territorial boundaries seems to vanish thus the concept of territorial jurisdiction as envisaged under s.16 of Civil Procedure Code of India and s.2 of the Indian Penal Code will have to take a path to alternative method of dispute resolution.

REASONS FOR THE GROWTH OF CYBER-CRIME IN INDIA

The main victim for this evil is unfortunately women or young teens both boys and girls. The study shows that 40 % of the Internet users in India are Women. It has been a common phenomenon that the important information of the net users is being disclosed time and again easily and is used for illegal purposes. The reason for the increasing cyber-crime in India against women can be studied in two fold aspect i.e. Legal Reason and Sociological Reason.

➢ Legal Aspect

The object of forming Information Technology Act is crystal clear that it was created mainly for enhancing e-commerce hence commercial as well as financial crimes i.e. hacking, fraud, and breach of confidentiality etc., but the drafters did not think about safety of net users. Majority of cyber-crimes in India are prosecuted under Section 66 (Hacking), Section 67 (publishing and transmitting obscene material in electronic form, Section 72 (breach of confidentiality. Cyber-crimes like cyber defamation, e-mail spoofing, hacking, cyber-sex and trace passing into one's privacy is very common now a days but I.T. Act is or expressly mentioning them under specific sections and provisions[15]. Whereas other Acts in India like Indian Penal Code, Criminal Procedure Code and Indian Constitution give special protection to women.

➢ Sociological Aspect

Due to hesitation and shyness of the victim and her fear of defamation of family name and impudence in the society, most of the cases of cyber-crime remain unreported in India. The victims always believe that they are more responsible for the crime done to her. Perpetrator's anonymous identity is one of the problem women are facing and is more susceptible to the danger of cyber-crime. The identity remains anonymous and the perpetrator may constantly blackmail or threaten with different names and identities. Another aspect is "character assassination", it is not totally wrong to say that women are significantly a favorite target for the society where she's expected to be suppressed. For the patriarchal society faulty behavior of a man is rather accepted and encouraged than to create deterrence for their acts.

CONCLUSION

The Indian society at large is torn between the dilemma of holding on to their twisted historical believes and the present day world. A faith that once denoted women as Supreme Power among all the deities today has all the reasons to put her under the radar and scrutiny of male society in order to satisfy their faulty ego. So much for dismay, A global poll conducted by Thomson Reuters in 2012 rated India as the "fourth most dangerous country" globally for women, and the worst country for women among the G20 countries[16]. The global jurisdiction of Internet causes a major threat to the society in the form of evil called Cyber-crime. ‘Vicious Net’ a very justified name is given to the current world of internet. Everywhere we can see a group of communities or an individual making fun of women irrespective of the status they hold in the society. Indian women are humiliated by their counterparts not only in real world, but in the ‘virtual world’ too. It has become quite a fashion to use the computer keyboard to undress a woman. Remember “Pen is mightier than sword” theory; people now are using this theory in digital fashion in most unwanted way. It is therefore crucial that there exist strong protections for the right to freedom of expression that balance state powers and citizen rights.[17]

References:

-http://www.thehindu.com/news/national/8-out-of-10-indians-have-faced-online-harassment/article19798215.ece

-U.S Commerce Department, “Falling Through the Net: Toward Digital Inclusion,” Washington, DC: U.S Commerce Department, October 16, 2000.

-Rohit Agarwal, Cyber Crime against women and regulations in India.

-Cyber Criminology : Exploring Internet Crimes and Criminal Behavior 285(K. Jaishankar ed., CRC Press : Taylor & Francis Group.)(2011)

-Cyber Criminology : Exploring Internet Crimes and Criminal Behavior 285(K. Jaishankar ed., CRC Press : Taylor & Francis Group.)(2011)

-Avnish Bajaj vs. State (2005)3CompLJ364 (Del), 116(2005) DLT427, 2005(79) DRJ576

-Oxford debates - http://freespeechdebate.com/discuss/privacy-free-speech-and-sexual-images-the-challenges-faced-by-legal-responses-to-revenge-porn/

-https://www.independent.co.uk/life-style/health-and-families/features/revenge-porn-enough-still-isnt-being-done-to-stop-it-9578892.html

-http://freespeechdebate.com/discuss/privacy-free-speech-and-sexual-images-the-challenges-faced-by-legal-responses-to-revenge-porn/

-Bernadette H Schell and Clemens Martin, Cyber Crime: A Reference Handbook, Contemporary World Issues Series 65 (ABC CLIO) (2004)

-News article referred as https://www.hindustantimes.com/india-news/cbi-approaches-40-countries-in-child-pornography-case/story-F12Oxd2HF3nCEHUMnIrR4O.html

-Published News Report - https://www.indiatoday.in/india/story/delhi-metro-fir-porn-clips-commuters-cctv-footage-delhi-police-169720-2013-07-09

-Abhimanyu Behera “Cyber Crimes and Law In India” XXXI, IJCC 19 (2010)

-http://www.freepressjournal.in/mind-matters/changing-role-of-women-in-india/238407

-https://cis-india.org/internet-governance/blog/freedom-of-expression-in-a-digital-age