Volume-11, No. 1 Feb.-2024, pp. Eng.11-17

Cyber Crime against Women

Dr. Ajeet Singh, Asstt. Professor,
Department of Political Science
Govt. P.G. College, Kotdwar Pauri Garhwal,
Uttarakhand India .

Introduction:
The traditional Indian society places women in a very high regards, the Vedas glorified women as the mother, the creator, 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 penalised. Cyber crime and internet bullying works in similar manner where the wrong- doers are not afraid of any authority that can penalise.

Main Words-

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.

Understanding Cybercrime:

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:

1. **Cyber Harassment**: Cyber Harassment is characteristic repetitive behaviour intended to disturb or up rest a person though use of internet. A particular class of harassment which is sexual in nature is known as sexual harassment, among several other things it majorly includes persistent and unwanted sexual advancement. Under Indian law sexual harassment has newly been defined under the Criminal Law Amendment (Bill) 2013 as physical contact and advances involving unwelcome and explicit sexual overtures; or

1. A demand or request for sexual favours; or
2. Making sexually coloured remarks; or
3. Forcibly showing pornography; or
4. Any other unwelcome physical, verbal or non-verbal conduct of sexual nature.

67 A, 67 B of the IT act provide sexual harassment in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, 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.

2. **Cyber Stalking**: Cyber Stalking basically is behaviour wherein an individual wilfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes that person. 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 may be considered less than four reasons,

1. Sexual harassment.
2. Obsession for love.
3. Revenge and hate.
4. Ego and power trips.

Ritu Kohli Case-

Ritu Kohli Case was India'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 add hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on add 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. This is first time when a case of cyber stalking was reported.

Similar to the case of email harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the IT Act that perpetrator can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again for outraging the modesty of women.

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

The DPS MMS scandal 3is 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 paedophiles. The Mumbai police arrested the couples for pornography4.

The most recent example is of Delhi Metro CCTV footage leaks case5, where the CCTV recording couples getting intimate in metro stations etc. which has been recorded by police security cameras has been leaked on internet.

Unlike other crimes like Cyber Stalking Cyber Defamation Morphing. Email Spoofing, Cyber Pornography is considered an exceptional case which has been covered by the IT Act 2000 to a certain extent by Section 67 of the IT Act 2000. Along with IT Act the perpetrator can be punished under various Sections of IPC (Section 290 for committing public nuisance, section 292 for sale of obscene books etc, and section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, section 293 for sale etc of obscene objects to young persons and then section 294 for doing or composing, writing etc of obscene songs and finally under section 509 for outraging the modesty of women).

4. **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 Kwatra6-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 SuhasKatti7-** 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.

5. **Morphing:** Morphing is editing the original picture so as to make it look completely or largely different. 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. Often the next step after this is to blackmail those women through the threat of releasing the morphed images and din blasting the status of these women in society.

The recent **Air Force Balbharati School case (Delhi) 8** is a recent case comes under this category where a student of the School was leased by all his classmates for having a pockmarked face. He, who of the School 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. Such acts can be penalised under L.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC sec 509 also.

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; it is done by properties of the email, such as the From, Return-Path and Reply-To fields, 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. are then used to blackmail those women. The most popular case of cyber spoofing is Gujrat Ambuja's Executive Case9, in this case the perpetrator pretended to be a girl for cheating and blackmailing the Abu Dhabi based NRI.

Reasons for the Growth of Cyber Crime against Women in India

The transcendental jurisdiction of Internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women and children. Studies shows that we have 52 million active internet users in India which reached at 71 million in the year 2009. Among them working women net users are 8% and 7% nonworking women in the year

2009 and 37% usage of all users accessing internet through cyber café10. It is very common occurrence that the essential data of the internet surfer is being released effortlessly by the owners of cyber café and then it is used for illegitimate dedications. Though acquaintance with technology is constructive facet that can be considered vital for the progress of any country but at the same time it is becoming the foundation to upsurge the offense rate with technology against the weaker sector of the society. Statistics also show that cyber awareness amongst people in India in really low.

Table 1: Awareness of cyber culture among Indian internet users

Awareness of cyber culture among Indian internet users	Yes %	No %
Knowledge of minimum age to join cyber communities like Facebook, Orkut, My space etc	56.2	43.8
Allow others to use one's own email id / profile id/passwords	46.6	53.4
Use safety tips like filtering emails, locking personal albums and information, personal walls of social networking sites etc;	69.9	30.1
Mail back to unknown senders of spam/pornographic/erotic/phishing mails.	37.0	63.0
Share personal information/emotions with virtual chat room partners etc whom you don't know in real life	74.0	26.0
Believe in controlling free speech while communicating in the cyber space	37.0	63.0
Read policy guidelines of social networking sites, ISPs etc:	28.8	71.1
Use pseudo names	45.2	54.8

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

Legal Reasons-

The objective of the IT Act is crystal clear from its preamble which confirms that it was formed largely for improving e-commerce hence it covers commercial or economic crimes i.e. Hacking, fraud, and breach of confidentiality etc. but the drafters were unacquainted with the protection of net users. As we deliberated above that majority of cybercrimes are being prosecuted under Section 66 (Hacking). 67 (publishing or transmitting obscene material in electronic form), 72 (breach of confidentiality). The most of the cybercrimes other than e-commerce related crime are being dealt with these three sections. Cyber defamation, cyber defamation, email spoofing, cybersex, hacking and trespassing into one's privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions11. Whereas IPC, Criminal Procedure Code and Indian Constitution give 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 and prosecuted under IPC. Indian constitution guarantees equal right to live, education, health, food and work to women, however until recently there were no specific penal provisions protecting women specifically against internet crimes. Ever since the 2012 Delhi Gang Rape case (Nirbhaya Case) there has been a huge outcry over bringing out new reforms and penal provisions so as to protect women against the criminally minded. The 2013 Criminal Law Amendment Ordinance contains several additions to the Indian Penal Code, such as to sections 354, 354 A, 354 B, 354 C & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner.

As it has been discussed earlier that transcendental nature of Internet is one of the main reasons for the growth of cybercrime so whereas Section 75 of the IT Act deals with the offences or contravention committed outside India but it is not talking 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. Although in the most of the cases, for the matter of territorial jurisdiction Criminal Procedure Code is being followed.

Sociological reasons-

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. The women are more vulnerable to the danger of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. 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.

Remedies-

1. The increasing numbers of crimes against women are a huge concern for any state however, cybercrimes make it even more challenging as criminals have the opportunity to create fake identities and then after indulge in illegal activities. To counter this government should make stricter laws to apply on the Internet Service Providers (ISP), as they alone have the complete record of all the data being accessed by anyone surfing on net. ISPs should be made to report any suspicious activities that any individual is indulging into, this will help to curb crimes in nascent stage.
2. Legislation needs to make stricter regulation for cyber cafes, who should keep a record of their customers who utilized their internet services, often people, go to cyber cafes to indulge in criminal activities so as their own IP addresses are not revealed in any future investigation. This is another manner to mask identity.
3. People need to be cautious over which parts of their daily lives are being recorded by cameras & should act modest in such times. Awareness over cyber culture and its back draws also need to be improved amongst people. People need to be made aware of their rights; studies show that a large population of internet users in India have no knowledge of their rights in such matters:

Awareness of rights and reporting behaviour	**Yes %**	**No %**
Aware that hacking, creation of pornography/distributing the same, distribution obscene materials etc are criminal offences	80.8	19.2
Aware of his/her legal right to protect privacy in the cyber space	78.1	21.9
Aware that cyber bullying, cyber stalking, sending annoying, defaming messages etc can be penalized	19.2	80.8
Has reported incidences of cyber victimization to police/lawyers /courts	9.6	90.4

4. Email spoofing is possible because of Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email,

does not allow an authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, however this precaution is not always taken.5 So women should take precaution and always add the SMTP service extension with the SMTP client.

What Victims Need to Do-

Unfortunately even today the Indian police tends to not tends to take cybercrimes seriously, in such scenario, the woman or the young girl who falls prey to cyber victimization should first contact a women assistance cell or NGO (such as All India Women's Conference12, Sakshi13, Navjyoti14, Centre for cyber victimscounselling15) 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. Though there used to be several difficulties in dealing with cybercrimes such as loss of evidence and lack of cyber army but with the Criminal law Amendment Bill (2013) most of these problems have been taken care. However, several changes are still needed such as cyber savvy judges.

Cybercrimes against women are still taken lightly in India, mostly because in general the respect towards women in our modern society is on a decrease also a lot of people are unable to come to terms with the fact that even posting images of someone online in a crime. Cybercrimes such as morphing, e-mail spoofing do-not have a moral backing in society and hence are taken lightly. This brings us to the most important part where social advancement is needed, people need to recognise the rights of others and realise 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 kinds 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. Student of Law at National Law University, Odisha. India
2. http://cyberlaws.net/cyberindia/2CYBER27.htm
3. http://en.wikipedia.org/wiki/DPS MMS Scandal
4. G. Rathinasabapathy and L. Rajendran, "Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007)
5. http://zeenews.india.com/news/nation/porn-mmses-from-delhi-metro-cctv-footage_860933.html
6. http://cyberlaws.net/cyberindia/defamation.htm
7. http://www.naavi.org/cl editorial_04/suhas_katti_case.htm

8. Abhimanyu Behera, "Cyber Crimes and Law In India," XXXI, IJCC 19 (2010)
9. http://www.indiaforensic.com/cyberextortion.htm
10. http://www.academia.edu/440672/Cyber victimization in India A baseline sur vey report 2010
11. Abhimanyu Behera, "Cyber Crimes and Law In India," XXXI, IJCC 19 (2010
12. http://www.aiwc.org.in/ (Private group of women assisting other less fortunate women to fight the crimes committed against them)
13. http://www.sakshingo.org/ (NGO assists women in dealing with govt authorities)
14. http://www.navjyoti.org.in/ (NGO by Kiran Bedi, assist women in several aspects)
15. http://www.cybervictims.org/(Private group of legal minded individuals who help the victims of cybercrimes)