The Increasing Trends of Cyber Crimes Against Women: An Indian Perspective

Dr. G. Mallikarjun[1]

[1] Assistant Professor of Law, NALSAR University of Law, Hyderabad.

Abstract

In virtual world of internet, the sharing of information is very fast and easy. Internet has become the fastest mode of information sharing tool in the present global world. The number of users of internet in India has been increasing day by day, not only in the metropolitan cities but also in the rural areas. There are numerous advantages with the internet, but at the same time it has become a major mode of instrument to commit virtual crimes against women anonymously. The cyber-crimes pose a great threat to the individual integrity and privacy. Cyber-crime is a global phenomenon and women are more vulnerable and susceptible to the cyber-crimes. Cyber-crimes and privacy breaches in India have been increasing day by day, more particularly against the women with an intention to cause psychological harm to them. Like cyber defamation, cyber-stalking, sending threatening messages, morphing of photos, and e-mail spoofing against women etc. Some of these crimes are rampant in India. The lack of knowledge and consciousness about the use of internet and the social media, the women in India are facing a great vulnerable threat to their lives and to their privacy. In this article, the author explores the issues relating to online security vulnerabilities and the cause of cyber-crimes against women.

***Key words**: Cyber-crime, Cyber- Stalking, Morphing of photo, E -mail Spoofing, Cyber law, Information Technology Act 2000, and women empowerment*

Introduction:

The rampant usage of technology and increased trends to access to the internet has created the good opportunities for the development of commerce, research, education, entertainment and public discourses. It is true that technology is a boon to mankind but misusing of the same has witnessed increasing incidence of Cyber Crimes in India and there is no proper protection or safe guards to the victims of cyber-crime more particularly women who are more prone to the cybercrimes. Cybercrimes are not only affecting the privacy of the individuals but also poses a threat to the security and integrity of the state or organization. The cybercrimes in India, though on rise, mostly go either unreported or conviction is very poor. Cyber-crime and privacy breaches in India have been increasing day by day, more particularly against women with an intention to cause psychological harm to them. Like cyber defamation,[2] cyber-stalking, sending threatening messages, morphing of photos, and e-mail spoofing against women etc. Some of these crimes are rampant in India. Therefore, in this paper an attempt has been made to understand the nature of the cybercrimes and its impact over the women rights and the security and integrity of the women in India.

[2] Defamation: Sec 499 of IPC Provision and IT Act 2000

Cyber-Crime: The Definition:

Cyber-crimes are the crimes committed with the use of computers or relating to computers, especially through the internet. Crimes which involve use of information or usage of electronic means in furtherance of crime are covered under the ambit of cyber-crime[3]. Cyber space crimes may be committed against persons, property, Government and society at large. The United Nations Congress divided the cybercrime into two categories and defined thus[4]:

a) Cybercrime in a narrow sense that is computer crime in which any illegal behavior have been done by the means of electronic operations that targets the security of computer systems and the data processed.
b) Cybercrime in a broader sense which is computer-related crime any illegal behavior committed by means of an operating system or network, including such crimes as illegal possession or distributing or altering any information by means of a computer system or network.

Therefore, Cyber Crime is a term that refers to all criminal activities done by using the computers or computer networks or by using other devices like mobile phones, tablets[5] etc. It also covers the traditional crimes in which computers networking are used to enable the forbidden activity. Cyber Crime can be categorized in three ways[6]:

1. **The computer as a target** – attacking the computers of others.

2. The computer as a weapon- Using a computer to commit "traditional crime".

3. The computer as an accessory- Using a computer as a "fancy filing cabinet" to store illegal or stolen information.

Cyber offenses specifically committed against women:

In the present pandemic situation though normal crimes have reported to have been come down but Cybercrimes against women are increased may folds. It is very much evident in the words of K. Indraveni, Joint Director, Centre for Development of Advanced Computing. She rightly observed while speaking to media that there was a significant increase in cyber crimes against women during lockdown. For that she referred to the data collected by the National Commission for Women, which shows that 54 cybercrime

[3] According to The Cambridge English Dictionary
[4] At the tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to cyber space cybercrime was divided into two categories.
[5] Kanika Chhabra and Gunjan Chhabra, A Study on Emerging Issue on Cyber Law, Advances in Computer Science and Information Technology (ACSIT), Volume 1, Number 3; November, 2014, Krishi Sanskriti Publications pp. 112-116, http://www.krishisanskriti.org/acsit.html, (Accessed on 23-10-2020)
[6] R. M. Johri , Principal Director (information Systems)Cyber Security – Indian Perspective, Office of CAG of India, see for further details *www.intosaiitaudit.org*

complaints were received online in April in the year 2020 in comparison last year's complaints received online by the April 2019 were only 37. Further, she observed that during the look down, there were 412 genuine complaints of cyber abuse from March 25 till April 25, 2020. Out of these, 396 complaints were serious in nature.[7]

Therefore, to understand the natures of cybercrimes which generally committed against the women, some of them discussed herein. However, the list of offenses given below is not exhaustive and would include many other offenses that would be committed through a computer or against a computer in the future.

1. Cyber Stalking:

Repeated acts of expressed or implied harassment or physical threat towards the victim through the internet. Even they use very filthy and obscene language to invite the interested persons. If the stalker is able to access the telephone of the victim, repeated calls will be made to the victim to threaten, harass, or intimidate them. Stalkers, generally, have desire to control the victims life. Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female[8]. Cyber Stalking is referred in the context when internet is used to know the likes/dislikes of the victim, her friends, etc and then use this personal information to create fake accounts elsewhere or to commit offence in physical world. Section 354D of IPC talks about this and includes the offence of cyber stalking in it.

In a recent court case, Yogesh Prabhu vs State of Maharashtra[9], the woman was chatting with a man on a dating/matrimony website and then stopped chatting with him. However, the man kept an eye on all her online profiles and then started sending her obscene images and video clips. She initially ignored him, but later lodged a complaint with the police. The trial began and the magistrate held the accused as guilty under Section 509, IPC(outraging the modesty of woman by using words, etc) and Sec 66E of IT Act(punishment for violation of privacy). This was due to the fact that the cyber stalking provision was included in Sec354D, IPC through 2013 amendment act and hence, could not be retrospectively applied to an offence occurred in 2009.

In Genpact BPO Case (Cyber stalking/cyber bullying)[10], a Female employee of Genpact was repeatedly harassed by the erstwhile employee of the same company with absence mails. She filed a complaint along with email copy consisting of email header by which IP address of the sender was traced and with that email address of the accused was found to be from rediffmail.com to send the said mails. A case was booked against him for Cyber stalking.

[7] https://www.thehindu.com/news/national/andhra-pradesh/cyber-crimes-against-women-on-the-rise/article32399536.ece (Accessed on 24-12- 2020)
[8] See http://www.nandedpolice.in/cyber.php, (Accessed on 13-11-2020)
[9] https://indianexpress.com/article/cities/mumbai/cyber-cells-first-conviction-man-gets-3-years-for-sending-obscene-messages-stalking-colleague/
[10] See http://gurgaon.haryanapolice.gov.in/case-studies.htm, (Accessed on 05-11-2020)

2. Cyber Harassment:

A harassment involving unwanted sexual advances or similar inappropriate behavior has been described as sexual harassment. If such harassment is done through online means, then it is known as online harassment or cyber harassment. Sexual harassment has been defined in Criminal Law Amendment Bill, 2013. Section 67A and 67B of Information Technology Act 2000, contemplated that the publication or transmission of content of sexual nature is crime and punishable. Email harassment is very similar to harassment through postal letters-yet it is difficult to trace the culprit due to the shield provided by the Internet.

A related crime which has become very popular these days is online trolling. Earlier the women were harassed physically but now they are threatened or blackmailed through online medium. In Saddam Hussain vs State of MP[11], the accused had outraged a woman by blackmailing her by sending a video in which she had some obscene gestures. A criminal complaint was filed in which the cyber offences involved were recorded under Sec.507, IPC (Criminal Intimidation), Section 66 of IT Act (this section was struck down by Supreme court in Shreya Singhal vs Union of India[12]), and various other offences like Stalking, etc. A petition was filed before the court for quashing on the basis of compromise between the parties. But the court refused the petition stating that the offence of cyber harassment and cyber stalking is an offence against the society and not against an individual. This shows that how seriously the judiciary has begun to consider the cyber-crimes against women. This is a welcoming step by the Judiciary in preventing the cyber crimes against women. In the case of State of West Bengal v Animesh Boxi[13], which is said to be the conviction of the first revenge porn case in India, the victim and the defendant were in a relationship during which the defendant acquired some the photographs of the victim, later started blackmailing her with them and posted them online to take revenge for ending their relationship. The offender was charged under S.66E, 66C, 67 and 67A of IT Act and S.354A, 354C, 354 and 509 of IPC.[14]

3. Cyber Pornography:

Cyber pornography is an offence committed when online/cyber medium is used to transmit and spread pornographic or obscene content. In physical world, the offence of pornography is dealt with Sec 292, IPC which deals with offence of obscenity. Also, Sec 354A, IPC inserted by 2013 amendment deals with obscenity, if a man is showing obscene material to a woman. These sections are very relevant for determining the offence of cyber pornography. When it comes to Information Technology Act 2000, Section 67A of the Act provides for prohibition of acts which include transmission of sexually explicit material through online

[11] 2016 SCC Online MP 1471
[12] (2013) 12 SCC 73
[13] C.R.M. No. 11806 of 2017, GR/1587/2017, cited by Aditya Krishna in his article titled "Revenge Porn: Prosecution Under the Current Indian Legal System, available at https://actionagainstviolence.org/revenge-porn-prosecution-under-the-current-indian-legal-system/?v=c86ee0d9d7ed (Accessed on 15-10- 2020)
[14] Ibid.

medium. A recent case in this regards is on Delhi Metro CCTV footage leak[15], where the CCTV recording of couples kissing in metros was leaked online on various websites. This raised question over the protection of privacy and the court ordered those websites to remove the videos and closure of some websites by the Government which were hosting those videos. Another landmark case in this regards is the DPS MMS scandal case[16], in which the sexually explicit MMS clip of a girl and boy was distributed on various internet websites. It would include pornographic websites; pornographic magazines produced using computer and the Internet (to down load and transmit pornographic pictures, photos, literature etc.)[17]

4. Cyber Defamation:

Just like in physical/real world defamation happens when the person's reputation or goodwill is tarnished (see Sec 499, IPC)- in online sphere, this offence happens when internet is used as a medium to tarnish the reputation or goodwill of a person.

One of the first cases which came in this regards is the SMC Pneumatics Ltd v Jogesh Kwatara[18]. In this case, one of the employees of the company tarnished the image and goodwill of the plaintiff company by sending emails on frequent basis. The court granted an ad-interim injunction order restraining the employee from doing so. The State of Tamil Nadu v Suhas Katti[19] is another prominent case in this regards. Here, the lady's email id and contact number was posted by the culprit on several websites and chat groups, and she used to receive phone calls at odd hours in night time. The people calling her were under the impression that she is soliciting sex services. Thus, her image and reputation was tarnished through this. The culprit was awarded rigorous imprisonment of two years and was fined.

5. Morphing:

Morphing means editing the image or picture/video of a user without any permission from the victim. Often the image or picture is super-imposed on a nude image or simply clad women and then uploaded on internet to tarnish the image of the girl. This is similar to defamation, except the fact that here, no statements are made; just the pictures or videos are circulated of the victim. News has been reported on actress, on frequent basis, that their pictures and videos are being morphed and circulated. Even minor girls and women are also victim of this nature of crime[20]. Air Force Bal Bharti School case(Delhi)[21] is a prominent case in which a student of the school morphed the images of his classmate and teacher and morphed them using nude images. He was booked under this offence and subsequently awarded punishment by the court.

[15] See https://www.indiatoday.in/india/north/story/red-faced-dmrc-to-probe-cctv-clips-leak-169758-2013-07-10
[16] Avinash Bajaj v State (2005) 3 CompLJ364 Del
[17] See http://www.cidap.gov.in/documents/cyber%20Crime.pdf, (Accessed on 13-11-2020)
[18] *SMC Pneumatics India Pvt. Ltd. v. Jogesh Kwatra*, CS(OS) No. 1279/2001 (Delhi High Court, 2001)
[19] https://www.legalserviceindia.com/lawforum/index.php?topic=2238.0
[20] Celebrities and Cyber Crimes: An Analysis of the Victimization of Female Film Stars on the Internet by Debarati Halder and K Jaishankar
[21] https://www.dqweek.com/net-pornography-incident-at-bal-bharti-school-raises-several-issues/

The offence is regulated by Sec 43(altering/destroying the data) and Sec 66(deals with computer related offences) of Information Technology Act 2000. Moreover, sections of IPC like : Sec. 354A (sexual harassment) , Sec290 (Public nuisance), Obscenity (Sec 292A) and Defamation (Sec 501) would also be applicable in case this offences occur.

6. Email Spoofing:

Sending offensive messages through an electronic communication so as to cause annoyance or sending an email to mislead or deceive the recipient about the origin of such messages are commonly known as IP or email spoofing[22]. In this way, by impersonating the identity of some other person, the email sender tries to extract some personal information.

Email spoofing would come under the preview of Section 415 IPC (cheating), Sec 416, IPC (cheating by Personation). It is to be noted here that the offence of cheating by personation is committed when the person's whose identity is impersonated the email is real or imaginary (person/corporation). Sec 66D of Information Technology Act 2000, deals with cheating by personation using computer devices or some aspect of Information Technology. This offence attracts rigorous imprisonment and fine. In Gujarat Ambuja's Executive case[23] the culprit pretended to be a girl and cheated an NRI based in Abu Dhabi.

Conclusion & Suggestions:

Laptops and smart phones have become a handy use for the people of the all age group and at the same time use of internet also increased. This shows the level of penetration of internet in each household. Even rural areas have shown an attraction towards using new technology. Thus, values of the society in physical life have now extended them to online life. Patriarchy and Misogyny are all pervasive in the Indian society which is the main cause in increasing crimes against Women, in both physical and online sphere. The transition to online life happened quite quickly in India. For this reason, people are still unaware of any rights and duties which they have while using the Internet. Criminals have started perceiving Internet as a safe haven for committing crimes against women, as they find a lot of profiles of women on social networking platforms like Facebook, twitter, etc and they think they would not be recognized. At the same time, the victim women, simply ignore the cyber offences committed against them-and hesitate to bring them to attention of police, etc. As more and more people are shifting to cities and foreign nations, etc so Internet is becoming a very important tool in communication. In coming days, it is predicted that India will have even more users of Internet. Thus, cyber-crimes (and especially, cyber-crimes against women) cannot be ignored. Finally, cyber-crimes, unlike physical day offences like murder, etc would continue to evolve and new type of crimes would be seen in near future, as technology is developing in very fast pace. The existing law, the Information Technology Act 2000

[22] Section 66A of IT Act 2000.
[23] https://www.indiaforensic.com/cyberextortion.htm

provisions relating to publishing of information which is obscene in electronic form (Section 67), Access to protected system (Section 70), Breach of confidentiality and privacy (Section 72) needed to be revised to fix the offenders based on the experience and less conviction rate. Thus it is a high time for India to update the Law on time to time by way of amendments in existing laws with a holistic approach towards Internet related crimes with an effective enforcement mechanism. Apart from amending the existing laws to effectively deal with cybercrimes committed against women and children, the process of filing complaints should be simplified drastically apart from instilling the confidence on the victims that their identity will be protected at any cost. Moreover, the law enforcement agencies should be sensitized about the various facets of cybercrimes against women and the entire redressal mechanism should be fast-tracked. Concerted efforts must be made by the Government and its agencies to raise legal awareness amongst all the stakeholders to prevent as well as punish such offences. Therefore, there is a need students about cybercrimes at school level which will not only enable their young impressionable minds to understand the dangers present in the virtual world but will also make them more empathetic towards others.