IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Research paper on cyber-crimes against women

C.H.Gayathri Devi, I.Pavankumar, P.Sailaja

KLUniversity.

INTRODUCTION

The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called 'cyberspace'. It has become a platform for a galaxy of human activities which converge on the internet. The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment etc.1 there is hardly any human activity that is not touched by the internet. Therefore, Internet has something to offer to everybody and in the process, it only increases and never diminishes. Cyberspace has bestowed many gifts to humanity but they come with unexpected pitfalls. Due to the anonymous nature of the internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing the aspect of the internet to perpetuate criminal activities in cyberspace. Furthermore, cybercrime does greater damage to society than traditional crime and is more difficult to investigate.

Over the last few years, cybercrimes have become more intense, sophisticated and potentially debilitating for individuals, organizations and nations. Law enforcement agencies are finding it difficult to check and prevent the crimes in the cyberspace because the perpetrators of these crimes are faceless and incur very low cost to execute a cybercrime whereas the cost of prevention is extremely high. Targets have increased exponentially due to the increasing reliance of people on the internet.

India has bypassed Japan to become the world's third largest Internet user after China and the United States, and its users are significantly younger than those of other emerging economies, India now has nearly 74 million Internet users, a 31 per cent increase over March 2012, the report says3 . Andhra Pradesh (undivided), Karnataka and Maharashtra have occupied the top 3 positions when it comes to cyber-crimes registered under the new Information Technology Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries. This clearly indicates that the impact of Information Technology is very profound. Both Society and the Technology are operating in a way so as to harmonize with the pace of each other's growth.

With boon comes the bane and thus the World of Information and Communication Technology (in short 'ICT') is no except ion to this rule. Along with abundant opportunities that it has brought about, there are also some challenges too. Broadly speaking, it has posed certain major concerns like privacy threat, over riding cultural impact, more reliance on technology, boycott of societal engagements, computer virus, malware, spam phishing and many more. One of the major challenges in this era of ICT is of an increasing number of cybercrimes taking place in the World today.

As per Indian Computer Emergency Response Team (CERT-IN), one cybercrime was reported every 10 minutes in India during 20174 . These statistics are quite alarming and therefore, merit focused and collective attention from Law Enforcement Agencies. It is evident from the data revealed by National Crime Record Bureau (NCRB) in year 2016, where in about 12,317 Cybercrime cases were reported in India which is 6 percent higher than 2015. According to the annual report released by the NCRB in 2016, with 762 cases, Bengaluru had the second-highest number of cybercrime cases among the metros, behind Mumbai with 980 cases. Other metros in the list were far behind, with Hyderabad recording 291 cases, Kolkata 168, Delhi 90 and Chennai 36. From 762 to 5,035, the numbers of cases have seen a sharp increase in Bengaluru. The increase in Mumbai is not so pronounced. Experts and officials have attributed the high reporting of cybercrimes in Bengaluru to higher incidences and greater awareness among residents, among other factors. "In the other metros, such a step was not even considered. The station also had all the powers of other stations and a wide jurisdiction.

Cybercrimes reported these days, it becomes important and imperative to enquire as to meaning of the term Cyber Crime, the categories of Cyber Crimes. Cyber-crime is a crime done with the misuse of information technology for unauthorized or illegal access, electronic fraud; like deletion, alteration, interception, concealment of data, forgery etc., Cyber-crime is an international crime as it has been affected by the global revolution in information and communication technologies (ICTs). The number of Cyber Crimes committed is increasing with each passing day, and it is very difficult to find out as to what actually a cyber-crime is and what the conventional crime is.

Cyber Crime against Woman

The traditional Indian society places women in a very high regards, the Vedas glorified women as the mother, the creator, and 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.

The use of cyberspace and its attendant features of anonymity continue to influence both positively and negatively on social, economic, cultural, and political aspects of every society. Nevertheless, while the cyberspace have provided secure tools and spaces where women can enjoy their freedom of expression, information and privacy of communication, the same benefits of anonymity and privacy also extend to those who employ ICTs for criminal activities and use the internet to commit violence against women. The use of mobile phones and internet to stalk, abuse, traffic, intimidate and humiliate women is palpable in developing countries including India. While, the Information Technology Act, 2000 which was amended in the year 2008, begins to deal with the problem, it does not explicitly deal with all cybercrime and cyber security issues on the person and specifically women.

Women are the worst victim of cyber-crimes; in an incident where a Delhi school student circulated a mobile video clip of two co-students having sex initiated a heated debate on right of privacy of women and even compelled authorities to ban mobile phones in educational institutions. Every second, one woman in India gets tricked to be a victim of cybercrimes and the online platform is now the new platform where a woman's dignity, privacy and security are increasingly being challenged every moment. Trolling, abusing, threatening, stalking, voyeurism, body-shaming, defaming, surveillance, revenge porn and other forms of indecent representation of women are rampant in the cyber world. In cybercrimes against women, the effect is more mental than physical while the focus of the laws ensuring women's security is more on physical than mental harm.

the National Crime Records Bureau (NCRB) of India does not maintain any separate record of cyber-crimes against women. Technology is the resource used by some perpetrators who target to defame women by sending obscene WhatsApp messages, e-mail, and stalking women by using chat rooms, websites, and worst of all by developing pornographic videos, mostly created without their consent, spoofing e- mails, morphing of images for

pornographic content by using various software's available online. Indian women are not able to report cybercrimes immediately as they are not really aware as to where to report such crimes or are not serious about reporting the same due to social embarrassment they don't want to face.

Cyber violence is undeniably the new emerging form of violence in the 21st century and cybercrimes the most challenging crimes of recent times. Cyber violence is any online behaviour that constitutes or leads to harm against the psychological, emotional, financial, and physical state of an individual or group. Cyber violence against women and girls (cyber VAWG) is a fairly new phenomenon that is becoming more and more pervasive. Cyber violence against women can be defined as any form of gender-based and sexual violence expressed through ICTs such as the Internet, mobile phones and video games.

Indian women are not able to report cybercrimes immediately as they are not really aware as to where to report such crimes or are not serious about reporting the same due to social embarrassment they don't want to face. There is no doubt that cybercrimes are easy to commit with very little resources, but the damage can be huge to the security of women. "Social media has helped to enhance freedom of expression, including access to information in many ways.

Some of the major well-known cybercrimes have put thousands of women into various health issues such as depression, hypertension and women suffer from anxiety, heart disease, diabetic and thyroid ailments due to e-harassmenta) Harassment by E- Mails / Cyber Stalking / Cyber Teasing / Cyber bullying / Cyber flirting. b) Cyber Defamation. c) E-mail spoofing/SMS spoofing/ Phishing. d) Morphing/ Hacking. e) Cyber pornography/ Obscenity/ Sexual defamation. f) Revenge porn/Non-Consensual Pornography.

The history of cyberstalking in India goes back to 2001, in a case where a woman Ritu Kohli11 complained of being stalked on the internet. Manish Kathuria, a man, used Kohli's name to engage in illegally chatting and the sending of obscene messages on the website www.mirc.com. 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. Ritu Kohli reported the matter to the police and the Delhi Police swung into act, traced the culprit and slammed a case under Section 50912 of the Indian Penal Code for outraging the modesty of Ritu Kohli. By the Criminal Law (Amendment Act), 2013, Cyberstalking has been specifically outlined as a punishable offence under Section 354D13 of Indian Penal Code

Cyber defamation affects the welfare of the community as a whole and not merely of the individual victim. It also has its impact on the economy of a country depending upon the information published and the victim against whom the information has been published. Section 67 of the IT Act deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs. However the IT Act does not cover cyber defamation specifically, therefore to seek remedy against cyber defamation the aggrieved party will have initiate proceedings under the provisions of IPC read with the provisions of IT Act, 2000.

In the first case of cyber defamation in India, SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra14 , the reputation of a corporate was being defamed by an employee of the plaintiff company by sending derogatory, defamatory, obscene, emails obscene, vulgar, filthy and abusive emails to its employers and also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The Hon'ble Judge of the Delhi High Court passed an ex-prate ad interim injunction observing that a prima facie case had been made out by the plaintiff.

Relying on the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners, the Additional Chief Metropolitan Magistrate held the accused guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/- and for the offence u/s 509 IPC sentenced to undergo 1 year Simple

imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently." The conviction of the accused was achieved successfully within a relatively quick time of 7 months from the filing of the FIR.

In March, 2018, a man in West Bengal was sentenced to five years imprisonment and fined Rs.9,000 for uploading private pictures and videos of a girl without her consent as revenge for ending their relationship.18 Under the promise of marriage, the accused pressured the complainant into providing explicit images of her, andleveraged his threats to upload these pictures onto social media to acquire more pictures. Later, he accessed her phone without her knowledge to retrieve more private pictures and videos. When the complainant refused to continue their relationship, he uploaded this material onto a popular pornographic website along with both her and her father's names. In addition to the defendant's imprisonment and fine, the State Government was directed to treat the victim as a survivor of rape and grant appropriate compensation. With evidence provided by service providers Reliance Jio and Google, the perpetrator was convicted under sections. 354A, 354C, 354 and 509 of the IPC as well as sections. 66E, 66C, 67 and 67A of the IT Act, in what is likely the first revenge porn conviction in India.

Although the National Crime Records Bureau documents cyber-crimes against women, there are no official statistics available that pertain specifically to revenge porn in India. A 2010 report suggests that "only 35 per cent of the women have reported about their victimization, 46.7 per cent have not reported and 18.3 per cent have been unaware of the fact that they have been victimized … women prefer not to report about their victimization owing to social issues."

A legal framework for the cyber world was conceived in India in the form of E- Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000 which was amended in the year 2008. The IT Act amends some of the provisions of our existing laws such as the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Though since 2000 the IT Act is in place in India for curbing cyber-crimes, but the problem is that still this statute is more on papers than on execution because lawyers, police officers, prosecutors and Judges feel handicapped in understanding its highly technical terminology. Moreover cyber-crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace.

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. The majority of cybercrimes are being prosecuted under Sections. 66, (Hacking), 66E,22 67 (publishing or transmitting obscene material in electronic form), Sec. 72 (breach of confidentiality). The most of the cybercrimes other than e- commerce related crime are being dealt with these three sections.

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) Act contains several additions to the Indian Penal Code, such as to sections.354, 354 A, 354 B, 354 C23 & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner. Again, under no section in IT Act 2000, Obscenity – personal viewing – Is an offence, in fact like in IPC section 292 again if it is proved that you have published or transmitted or caused to be published in the electronic form only then under Sec. 67 it can be an offence. Last but not the least, the IT Act 2000 does not mention the typical cyber-crimes like cyber stalking, morphing and email spoofing as offences.