International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 6(C); June 2018; Page No. 13307-13311
DOI: http://dx.doi.org/10.24327/ijcar.2018.13311.2366

Research Article

WOMEN HARASSMENT THROUGH CYBERSPACE

Gayathri P*

Sri Sakthi Nagar, Arumbakkam Chennai 600106

A R T I C L E I N F O

Article History:

Received 8th March, 2018
Received in revised form 24th April, 2018 Accepted 16th May, 2018
Published online 28th June, 2018

A B S T R A C T

The cyber-crimes pose a great threat to individuals and society. Cyber-crime is a global phenomenon and women are the soft targets of this new form of crime. Cyber-crime is emerging as a challenge for national and economic security. Cyber Stalking, Harassment via Email, Cyber Defamation, Morphing, and Email Spoofing against women are some of the various forms of threats faced by women in cyber space.
India is considered as one of the very few countries to enact IT Act 2000 to combat cyber-crimes. This Act is widely covered commercial and economic crimes which is clear from the preamble of the IT Act but it is observed that there is no specific provision to protect security of women and children. However there are few provisions to cover some of the crimes against women in cyber space under IT Act. Indian women netizens are still not open to immediately report the cyber abuse or cyber-crime. This nature provides the offenders the chance to escape after the commission of cyber-crime. The problem would be solved only when the victimized woman then and there report back or even warn the abuser about taking strong actions.

INTRODUCTION

Cyberspace has now become a global phenomenon and has become a problem for all nations. There are billions of people who frequent the cyberspace everyday be it for professional, personal or social reasons. Almost every second household has access to the internet. With nearby two billion internet users worldwide there are greater opportunities to entrap new victims, including women and children. New information technologies are being used to commit heinous crimes.[1]

Various forms of Cyber Crime against Women

Cyber Stalking

Exponential advances in the field of information technology have led to easy victimization. Stalking according to the dictionary means to pursue or approach, prey stealthily. Cyber stalking is the stalking of any person online. In case of cyber stalking of women it means that the stalker follows her all over the net be it chat rooms, social networking websites and make life hell. There have been cases of cyber stalking which have let to cases of rapes, acid attacks and in many extreme cases murder and robberies. Cyber stalking or technology aided stalking has only been recently been recognized as crime.

Corresponding author:* **Gayathri P
Sri Sakthi Nagar, Arumbakkam Chennai 600106

Internet predators have easy access to victims through facebook.com and myspace.com. Since very little empirical work has been done in this field it is not easy to draw statistics. Many women have to live in constant fear because of being stalked online by men who are sick.[2]

There are two types of cyber stalking:

- Online cyber stalking starts on the net and stays online.
- Cyber stalking starts on the net and continues offline where the stalker manages to get the woman's phone number or address and then troubles her.

There have been 966 cases reported of cyber crime in 2010 under the IT Act 2000. The people behind cyber stalking are mostly jilted lovers, perverts and pedophiles.

Example of cyber stalking via technology include:

- Sending threatening or unwanted emails, Instant messages (IM), beeper messages or cell phones text messages.
- Using a person's email address to subscribe him/her to multiple lists or to purchase goods/services in his/her name.
- Stealing a person's online identity to post false information. Sending misinformation to chat rooms, using net groups or lists to humiliate someone and/or encourage other group members to harass another individual.

[1] G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007).

[2] Dr.Astha Bhanot,Gender Violence, Pointer Publications, Jaipur (2013) pg.26.

- Posting a person's demographic information or photograph on pornographic sites.
- Accessing, monitoring and manipulating a person's computers while he/she is online.
- Accessing bank accounts, student's registration, telephone accounts and other personal data available online.
- Developing a website in 'tribute' to a person.
- Compiling online demographic information with intent to harass, threaten or harm a person with online/ offline
- Tracking a person through illegal wire tapping, caller identification, cameras, global positioning systems or other tracking devices.[3]

Harassment through E-Mails

Harassment through e-mails is no different from harassment through mails. In this women are threatened, blackmailed, bullied and cheated by emails. Men make fake email ID's and blackmail women by sending them their morphed pictures and threaten them to make it go viral if the women do not give in to their demands. There are spam mails that are sent to women and they contain viruses and worms like Trojan, love bug etc. There are some viruses that can attack the computers and extract all the personal details stored in it. People also tamper with the computer source code which is again a copyright violation.

Harassment by making Fake IDs

Another form of cyber crime that is on the rise lately is wherein men make fake id's of the woman concerned on social networking sites or make their fake mail accounts and the use morphed pictures which they post on the net or send through the email account to any number of people.

Online Pornography

Pornography is any form is a problem for women and children. There are a large number on porn sites on the net. These sites thrive on internet traffic. Many times women are not even aware of the fact that their photographs are on such sites. A large number of cases have been reported where people have morphed and doctored pictures of women and put them on porn sites. Pornography is a systematic practice of exploitation and subordination which dehumanizes women.

Misuse of Social Networking Sites

Now-a-days a large number of cases are reported in the police station everyday where the women are harassed to such a point by men who have morphed their pictures and made fake id's in their name and put up all their personal details on the net. Cases have been reported that men have put the woman's phone number on the net and she has been harasses by perverts. Many times people post fake photos on the social networking sites and link it to porn sites. They also post the girl's phone number and she is constantly harassed by men who are in access to the numbers.

Financial Cyber Crimes

Women have been duped on the net by people posing as financial consultants who take in all their financial details and then rob them of their money. Emails stating that the receiver has received a gift prize of sum of money lures naïve females into give their bank account details. Data theft also has become very common 24yr old Nadeem Hamid Kashmiri employee of HSBC BPO allegedly accessed personal information, security information and debit card information of some customers and these details were passed on to fraudsters who then diverted Rs.2crores approx from the clients' accounts. The victims of financial cyber crimes can be male and females both but in some cases it becomes easy for the person to get all the financial details out from the females by posing to be their friend.

Fraud on Dating Websites

Men on the prowl look for vulnerable women who are looking for love and are easy target of such people. They start by befriending the female and extracting all their personal details. There have been innumerable cases where women have met guys on dating sites and then have been raped and in worse cases murdered by them. Dating websites are a boon for the psychopaths. Women fall easy prey to these psychopaths and are lured into a vicious web wherein they fall for them and give them all their personal information. Serial Killers also frequent the web as they can hide in the anonymity and it is not easy to track them down. Very rarely are these psychopaths caught.

E-Mail Spoofing

E-mail spoofing is 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. Because core SMTP doesn't provide any authentication, it is easy to impersonate and itself into the person's computer triggers the virus.[4] Any mails sent forward to the other person's to whom the mails are sent. A worm can employ various methods of transferring the data.

Some Reported Cases on Cyber Crime

Cyber Stalking

Manish Kathuria Case[5]

There is a case of Mrs.Ritu Kohli. She complained to the police that a person was using her identity to chat over the internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days. She also complained that the person was chatting on the net using her name and giving address and phone number and was talking in obscene language. Mrs.Kohli received about 40 such calls in the span of 3 days from places like Kuwait, Cochin, Bombay and Ahmedabad. Delhi police traces the IP addresses to a Manish Kathuria. He pleaded guilty and was arrested under section 509 of the IPC nothing in the IT Act.

In June 2000, a man was arrested by the Delhi Police for assuming the identity of ex- employer's wife and distributing her phone number. When the victim reported to the police that

[3] Harvey, D "Cyberstalking And Internet Harassment: What The Law Can Do" available on GJRIM Vol 4, No 1, June 2014 46 http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_cyberstalking.pdf

[4] https://blog.malwarebytes.com/cybercrime/2016/06/email-spoofing/ retrieved on 02/10/2016.

[5] P Shah, Cyber staliking & the Impact of its Legislative Provisions in India, http://www.legalindia.in/cyber-stalking-the-impact-of-its-legislative-provisions-in-India (Last visited on 02/10/2016).

she was getting obscene calls in the middle of the night the police located the accused in the online chat room and then traced him by the telephone line used by him to access the internet.

Blackmailing

A Dubai based NRI was lured by an anonymous man on the internet who after winning her love started blackmailing her. He also sent fake copies of the love letters to her friends. Charges were framed under section 292, 389, 420, 465, 467, 468, 469, 474 IPC and section 67 of the IT Act.

Cyber Defamation

A Company's employee started sending derogatory, defamatory and obscene emails about the company's female Managing Director. The emails were anonymous and frequent and were sent to many of the company's business associated to tarnish the image and goodwill of the Company. The accused was later identifies by hiring a Private Computer Expert. Delhi High Court granted an injunction and restrained the employee from sending, publishing and transmitting emails which were defamatory to the plaintiffs.[6]

Obscenity

Some unknown persons had created an email id using the name of a lady and using her email id to post messages on five web pages describing her as a call girl with her contact numbers. Investigation was carried on the Chennai Police where the IP address and the ling details obtained from ISP were traced to two cyber cafes in Mumbai. Complainant received that she had refused a former college mate who had proposed to marry her. The police arrested this person and on examining his sim card found the complainant's number and the owner of the cyber café also identified this man. A charge sheet was filed U/S 67 of the IT Act 2000, 469 and 509 IPC. The accused was sentenced to 2 years of rigorous imprisonment. (State of Tamil Nadu v. Suhas Khatti, Egmore, Chennai 2004)[7]

Crime without Borders

Criminal enterprises benefit from the relative anonymity that the internet provides. With the strategic use of ISP by the criminals it becomes very difficult for the law enforcement to tackle them down as they relocate their ISP when they come to know that some law enforcement agencies are tracking them. These criminals sometimes work alone and in some cases they work in gangs. The major source of online exploitation is images of women where individuals pay some fee to access these sites. Other platforms are image-sharing sites, free hosting platforms and hacked websites. The less formal peer to peer networks do not leave a money trail and so it becomes difficult to track them down.

International Scenario

At the international level Article 6 of Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW)[8] convention urges States Parties to take all appropriate measures, including legislation, to suppress all forms of traffic in women and exploitation of prostitution of women. Beijing Declaration of women also highlighted the issue of technology and women. Declaration pointed out that the continued projection of negative and degrading images of women in media communications – electronic, print, visual and audio – must be changed. Print and electronic media in most countries do not provide a balanced picture of women's diverse lives and contributions to society in a changing world. In addition, violent and degrading or pornographic media products are also negatively affecting women and their participation in society.

Indian Legislative and Judicial Framework

The term 'pornography' when used in relation to an offence is not defined in any statutes in India but the term 'obscenity' has been effectively explained in two statutes in India, and these legislations prescribe that 'obscenity' in certain circumstances constitutes an offence.[9] These legislations are

- The Indian Penal Code, 1860 (IPC) and
- The Information Technology Act, 2000 (IT Act)

Section 292 of the IPC comprehensively sets out the circumstances in which 'obscenity' and/ or any 'obscene' material is an offence. According to section 292,

1. "Whoever sells, let to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation, or figure or any other obscene object whatsoever or
2. Imports, exports or conveys and obscene object for any of the purposes mentioned in (i) above, or knowing or having reason to believe that such obscene object will be sole, let to hire, distributed or publicly exhibited or in any manner out into circulation, or
3. Takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes mentioned in (i) above, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation or
4. Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under section 292 or that any such obscene object can be procured from or through any person or
5. Offers or attempts to do any act which is an offence under section 292, is punishable with imprisonment and fine. Therefore, obscenity is an offence if it falls within any of the above prescribed purposes.

Section 292 also sets out the purposes under which obscenity is not deemed to be an offence and these are when any such material is used

[6] The Times of India, Dec 18 (2010) "Cyber defamation increasing in India available on http://articles.timesofindia.indiatimes.com/2010-12-18/security/28256203_1_cyber-defamation-blog-sites-mega-housing- project

[7] The case of *Tamil Nadu* v *Suhas Katti* is worth mentioning for the fact that the conviction was successfully achieved within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial is applaudable.

[8] http://www.un.org/womenwatch/daw/cedaw/ retrieved on 02/10/2016.

[9] Law, Technology and Women: Challenges and Oppurtunities, Reference Press, New Delhi [2010], Pg.206.

1. Justifiably for the public good for e.g. interest of science, literature, art or learning or other purposes of general concern
2. In any Ancient Monuments and Archaeological Sites and Remains Act 1958 or in any temple, or on any car used for the conveyance of idols.

From a plain reading of Section 292 of the IPC it appears that if a person is in mere possession of the obscene material for his personal use without any intention to perform any of the purposes specified in section 292 it may not be an offence under section 292. In the case of

Jagdish Chawla & Others v. The State of Rajasthan[10]

The accused was caught viewing an obscene film on the television with the accused was caught viewing an obscene film on the television with the help of a VCR which along with the cassette was seized and a case under section 292 of the IPC was registered. The accused filed a petition in that simply being in possession of a blue film could not make a person guilty under section 292 unless it was further proved that the purpose of keeping the same was selling or letting it on hire. However it would be prudent to be aware that a prosecution may lie for mere possession of obscene material which may be for his own personal use, actually aids and abets the publication, sale, hire, distribution etc of the obscene material, which is an offence under section 292. And under section 111 of the IPC, the abettor is held to be equally guilty of the offence which he has abetted provided it is proved that the offence is a probable consequence of the abetment.

Obscenity under the Information Technology Act, 2000

Section 67 of the IT Act lays down the law that obscenity is an offence when it is published or transmitted or caused to be published in any electronic form. The expressions, 'publishing' or 'transmission' have not been specifically defined under the IT Act, but the commentaries suggest that 'publishing means making information available to people'. Transmission may be addressed to an intended recipient for his personal use. But that is not relevant. The act of 'transmission' is sufficient to constitute an offence under section 67 of the IT Act.

Therefore if any obscene material is published or transmitted in any electronic form it is an offence under section 67 of the IT Act. The transmission' and not mere possession of obscene information is an offence. The provisions of section 67 of the IT act are therefore similar to section 292 of the IPC where mere possession of the obscene material for one's own personal use may not be construed as on offence, However, it would be advisable to be cognizant of the fact that the prosecution can take a plea of abetment in a case of mere possession.

In the context of cybercafés in particular, if a customer downloads any obscene material for his personal viewing on the terminal assigned to him and this fact is known to the owner of the cybercafé would be liable under section 292 of the IPC read with Section 67 of the IT Act. Provided however, if it is established that this act was without the knowledge of the owner of the cybercafé it could be difficult for the prosecution to sustain its plea under section 292 and section 67 of the IT Act.

The law relating to the liability of cybercafé owners under these provisions of the IPC and the IT Act is not very well settled and therefore open to subjective interpretation. To mitigate liability and to avoid possible criminal prosecution the cybercafé owners could perhaps make an attempt to take protection under section 79 of the IT Act which absolves 'intermediaries', who only provide access to content but do not provide content itself, by extending the argument of intermediaries to cybercafés (although not tested in courts in India). The grounds of defense could be also made stronger by setting up a mechanism (hardware or software) whereby the customers are prevented from accessing any obscene websites and disclaimers are displayed prominently informing customers that obscenity is an offence which is punishable with imprisonment and that despite the warning, if customers still view such websites, they will be personally responsible and not the owner of the cybercafé.

Under the circumstances, the law as it stands on obscenity with regard to the liability it imposes on the owners of cybercafés is certainly not free from doubt and casts an onerous obligation on them to successfully defend a prosecution under the relevant provisions of the IPC and the IT Act. However, if certain precautions are observed such as establishing mechanisms which block such websites and displaying the disclaimers as suggested above, prominently, at least may help in providing a good defense. Regarding the punishment if we analyze the sections under 292 of the IPC for the first conviction a term of imprisonment (simple or rigorous) which may extend to two years, and with fine which may extend to two thousand rupees, and in the event of a second or subsequent convictions, with imprisonment (simple or rigorous) for a term which may extend to five years, and also with fine which may extend to giver thousand rupees. The punishment for an offence under Section 67 of the IT Act is on first conviction with imprisonment (simple or rigorous) for a term which may extend to one lakh rupees and in the event of a second or subsequent convictions with imprisonment (simple or rigorous) for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

CONCLUSION

The biggest problem in cases of cyber crime lies in modus operandi and the motive of the criminal. The Law enforcement agencies and the Judiciary have to keep up with the latest agencies and the judiciary has to keep up with the latest developments in the IT field in order to keep track of these crimes. Effective enforcement of laws is complicated by the transnational nature of cyber crimes. The UN Convention against Transnational Organized Crime[11] covers the most common forms of computer related crime because all these crimes are mostly transnational, involve criminal groups and are committed with the intent to achieve a material or financial benefit.

Along with this protocol to prevent, suppress and punish trafficking in persons especially women and children is relevant to the misuse of technology to abuse and exploit women and children. In India the law to protect women from cyber crime is in the Information Technology Act, 2000. Unfortunately even though chapter XI of the Act deals with offences such as tampering with computer source documents

[10] https://indiankanoon.org/doc/170577355/ retrieved on 02/10/2016.

[11] General Assembly resolution 55/25 of 15 November 2000.

(s.65), Hacking with computer system (s.67), Access to protected system (s.70), Breach of confidentiality and privacy (s.72), the Information Technology Act still needs to be modified. It does not specify any crime specifically as against women and children.

The IT Act 2000 does not mention the typical cyber crimes like cyber stalking, morphing and email spoofing as offences. Indian women are also not open to the idea of reporting cyber abuse. The general problem with any case of cyber crime like loss of evidence, lack of cyber savvy judges acts as a hamper. Still with the advancement of technology, the policies also becoming tech savvy wand with time they will be able to deal with it effectively. Cyber harassment is frightening for any women. It affects her freedom of movement and speech. There have been a lot of cases where the women have been forced on the brink of committing suicide and in some cases they have committed suicide. When a woman has being raped or when there has been an acid attack, the woman has to live with the social stigma and each day is a trial for them. Living a life is a torture and harassment for them. The enforcement agencies have to take it a little more seriously and have to realize that it has a damaging affect psychologically as well as physically on the woman who is subjected to it.

In this Age of information the 'virtual world' reigns supreme and it shapes our political, social and cultural outlook. Online abuse does not stay limited to cyberspace only. Shying away or going offline will not be able to solve the problem. Law enforcement agencies have to realize the gravity of the situation and frame laws accordingly and they have to realize the fact that the victims of online exploitation must live with their abuse for the rest of their lives. We all dream of living in Utopia but in order to reach their everyone has to work towards it. The whole scenario of cyber victimization is very complex and in the absence of empirical date it becomes very difficult to prove it. Cyber victimization is a violation of the fundamental rights and is gender harassment. A detailed study has to be carried out in this area so that the government can come up with proper laws for cyber crimes.

How to cite this article:

Gayathri P (2018) 'Women Harassment Through Cyberspace', *International Journal of Current Advanced Research,* 07(6), pp. 13307-13311. DOI: http://dx.doi.org/10.24327/ijcar.2018.13311.2366

****