IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138
INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CYBER-CRIME AGAINST WOMEN AND INDIAN LAW

Dr. Priti Atrey[1]

[1] Dr. Priti Atrey, *Associate Prof. Economics*, Mahila Vidyalaya Degree College, Satikund, Kankhal, Haridwar (Affiliated to H.N.B. Garhwal University, (A Central University) Srinagar (Garhwal) Uttarakhand)

ABSTRACT

The paper has two main sections, which tells about different aspects related to cybercrime against women in India. In first section we try to understand the cybercrimes committed against women as a whole. And second sections highlight prevention of cybercrime and government laws and policies related to it. Today world become global village through cyber networking and it became an integral part of human life. On the negative side, cyber networking has spawned new breeds of crime which is known as cybercrime. Research reveals that over the year the cybercrime has increased by 63.7 percent. Cyber related crime has a dark street, where there are many different types of crime that committed against women, are as- cyber stalking, online harassment through e-mail, cyber pornography, defamation, morphing, e-mail spoofing etc. Cybercrimes are dangerously increasing these days. In this background urgent need to understand its implications in prediction, prevention, detection and investigation on cyber related crimes and maintenance of law and order. So, this paper is completely focused on cybercrime issue, trends and problem faced by women and how cybercrimes can be minimized by formulating effective cybercrime laws in India.

KEYWORD- Cybercrimes, cyber stalking, online harassment, cyber pornography, defamation, morphing e-mail spoofing.

INTRODUCTION

Today world become global village through cyber networking and it became an integral part of human life. The online interactions have no geographical boundaries. Cyber networking site provide the many facilities like interaction, uploading information, pictures and videos for sharing. Smartphone have added a new dimension in cyber networking. In present days cyber networking services have become highly popular among the all-age groups of society in all over world.[i] On the negative side, cyber networking has spawned new breeds of crime which is known as cybercrime. Research reveals that over the year the cybercrime has increased by 63.7 percent.[ii] Cyber-crime is a global phenomenon and women are the soft targets of this new form of crime.[iii] Cyber related crime has a dark street, where there are many different types of crime that committed against women. In this background urgent need to understand its implications in prediction, prevention, detection and investigation on cyber related crimes and maintenance of law and order.

OBJECTIVES OF THE STUDY

The main objectives of the present paper are as under:

- To understand the different aspects of cybercrime committed against women.
- To highlight the cybercrime related laws of India and suggest the prevention related to cybercrime.

CYBER CRIME

Cybercrime or computer-oriented crime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense. Cybercrime may be referred to as computer crime.[iv] According to the Information Technology Act, 2000, 'cyber' may be said to include a computer, computer system or a computer network. Hence, any illegal act which involves a computer, computer system or a computer network is cybercrime (Barman.2015).[v]

WOMEN RELATED CYBER CRIMES

Cybercrime is a global phenomenon. With the advent of technology, cybercrime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. Though crime against women is on a rise in all fields being a victim of cybercrime could be most stressful experience for a woman. Especially in India where the society looks down upon the women and the law doesn't even properly recognize cybercrimes. The number of cybercrime cases reported across India in 2014 was a little more than 9,600. In 2013, the number was 5,693. Estimates for 2015 put the

[1] Dr. Priti Atrey, *Associate Prof. Economics*, Mahila Vidyalaya Degree College, Satikund, Kankhal, Haridwar (Affiliated to H.N.B. Garhwal University, (A Central University) Srinagar (Garhwal) Uttarakhand)

number of cybercrimes at 16,000[vi]. About 27000+ cybercrimes reported in 2017 with an average of one every ten minutes.[vii] In order to protect yourself from cybercrime, you need to know about the different types of cybercrimes committed against women. Here are different types of crime that committed against women, are as follows: -

CYBER STALKING

Cyber stalking or Harassment through e-mails is one of the most talked about net crimes in the modern world. Harassment includes blackmailing, threatening, bullying, and even cheating via email. Most victims of this crime are women. Cyber stalking has now spread its wings to social networking. With the increased use of social media such as Face book, Twitter and YouTube, your profile, photos, and status updates are up for the world to see. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites and email.

India's First Case of Cyber stalking was registered by the Delhi Police in 2001.[viii] Ritu Kohli Case[ix], The perfectly normal married life of Ritu Kohli, turned upside down, when she started receiving a number of emails from an unknown source (Mukut 2012).[x] Stalker used obscene language and posts her residence telephone number with other personal details on various websites, inviting people to chat with her on the phone. Kohli lodged a police complaint. Fortunately, Delhi police traced down the IP address of the hacker to a cyber cafe. The cyber stalker- Manish Kathuria, later got arrested by the police and was booked under sec 509 of the IPC and also under the IT Act of 2000 (Agarwal and Kaushik, 2014).[xi]

CYBER DEFAMATION

Cyber 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 Kwatra[xii] - cyber defamation was reported when a company's employee started sending 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.

HACKING

In hacking you are not able to login to your account. Someone who has changed email id or password and have taken complete control over your account. The meaning and scope of hacking under section 66 of the IT Act, 2000 is beyond than the mere 'illegal or unauthorized accesses but that should have been done fraudulently and dishonestly.[xiii] Face book is the most hacked social networking site.

CYBER PORNOGRAPHY

Cyber pornography is the other threat for female internet user. According to the Indian Constitution, largely, pornography falls under the category of obscenity and is punishable by law.[xiv] The DPS MMS scandal[xv] is a very famous case of this where an MMS clip of a school girl 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 on websites. The Mumbai police arrested the couples for pornography (Rathinasabapathy and Rajendran,2007)[xvi]. The most recent example is of Delhi Metro CCTV footage leaks case[xvii]. Which has been recorded by police security cameras has been leaked on internet.

MORPHING

Morphing is editing the original picture by unauthorized user or fake identity. It was identified that female's pictures are downloaded by fake users and again re-posted/uploaded on different websites by creating fake profiles after editing it. In Avnish Baja v. State, the petitioner was the Managing Director of the website Bazee.com which was an online shopping forum. A seller placed on the website a listing offering an MMS video clip for sale. To avoid the filter's, he placed the listing in the category of books and magazine. The item description was "DPS Girl having fun". A complaint was made to the website owner and after 2 days of the complaint the website wrote to the seller that the content has been removed due to the violation of user agreement (Barman.2015)."[xviii] The recent Air Force Bal Bharati School case (Delhi)[xix] is a recent case comes under this category.

E-MAIL 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. E-mail spoofing is then used to blackmail those women. The most popular case of cyber spoofing is Gujarat Ambuja's Executive Case[xx], in this case the perpetrator pretended to be a girl for cheating and blackmailing the Abu Dhabi based NRI.

CYBERCRIME RELATED LAWS IN INDIA

India is considered as one of the very few countries to enact IT Act 2000 to combat cyber-crimes; This Act widely covers the commercial and economic crimes (Jeet 2012).[xxi] Even though issues related to women still remain untouched in this Act (Agarwal and Kaushik, 2014).[xxii] Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cyber-crime. In general, they are used to book the perpetrators along with Section 292A of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, and under Section 509 of the IPC for uttering any word or making any gesture intended to insult the modesty of a woman.

According to Section 67 of the IT Act 2000, any person who sends, by means of a computer resource or any communication device any offensive information, shall be punishable with imprisonment for a term which may extend to three years and with fine (Didwania 2013).[xxiii] The offence of cyber defamation is well explained in the IPC under Section 500 which mentions punishment with simple imprisonment that can be extended up to two years or with fine or with both (Agarwal and Kaushik, 2014).[xxiv]

Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008. Some of the main features of the Information Technology Amendment Act 2008, which was effective from 27 October 2009, are as follows:[xxv]

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

Thanks to ITAA, Section 66 is now a widened one with a list of offences as follows:[xxvi]

- 66A Sending offensive messages through communication service, causing annoyance etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine.
- 66B dishonestly receiving stolen computer resource or communication device with punishment up to three years or one lakh rupees as fine or both.
- 66C Electronic signature or other identity theft like using others' password or electronic signature etc. Punishment is three years imprisonment or fine of one lakh rupees or both.
- 66D cheating by using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupee.
- 66E Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.
- 66F Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization
- Section 67 deals with publishing or transmitting obscene material in electronic form.
- Section 67-A deals with publishing or transmitting of material containing sexually explicit act in electronic form.
- Child Pornography has been exclusively dealt with under Section 67-B. Screening video graphs and photographs of illegal activities through Internet all come under this category, making pornographic video or MMS clippings or distributing such clippings through mobile or other forms of communication through the Internet fall under this category.

National Cyber Security Policy 2013 aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

Objectives of National Cyber Security Policy 2013 are as-[xxvii]

- To create a secure cyber ecosystem in the country,
- To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.
- To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy.
- To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management.

PREVENTION OF NETWORKING RELATED CRIMES

To deal with the situation of networking related cyber crime effectively, one needs to establish multi-dimensional public-private collaborations between law enforcement agencies, the information technology industry, information security organizations, internet companies, and financial institutions. If you are currently using networking websites, some prevention you will follow to protect yourself from online crimes are as following because prevention is better than cure.

- Log out every time you login from a device that is unfamiliar to you or not in use.
- Ensure that your password is a mixture of words and special characters. Don't have the same passwords for various social media accounts. Never store passwords, pin numbers and even own address on any mobile device.[xxviii]
- Face book has strong privacy settings which protect your account and things you share on it. Don't add strangers, people who are mutual friends (unless and until you know them). Identify fake profiles or pages that are sending you request or asking you to follow them.
- To keep your profile safe, you shouldn't allow people to see photos tagged by your friends, you can have control over them and take a call on photos before it goes all public.[xxix]
- Don't accept friend requests from random people. Don't reply to messages to people who are not in your friend list.[xxx]
- If the fraudster is calling you to some place, alone to give you something or asking you to go on a date then don't go.[xxxi]

- Don't transfer your card or bank details with anybody at any cost. If somebody is threatening you, report about it to the police. [xxxii]
- Don't strip or send your nudes through digital. [xxxiii]
- A fake profile on Face book will not use their genuine pictures (Having said this there are people who takes photographs of other genuine people as their profiles are public and use it to create a fake profile), they don't have many friends, and their profiles are just recently built. [xxxiv]
- Computer users must use a firewall to protect their computer from hackers. Computer users are recommended to purchase and install anti-virus software.[xxxv]
- Make sure that social networking profiles such as Face book, Twitter, YouTube are set to private. Check their security settings and be careful what information users post online. Once it is on the Internet, it is extremely difficult to remove.[xxxvi]
- Users must be alert while using public Wi-Fi Hotspots. While these access points are convenient, they are far from secure. Avoid conducting financial or corporate transactions on these networks.[xxxvii]
- Secure your Mobile Devices: Many people are not aware that their mobile devices are also vulnerable to malicious software, such as computer viruses and hackers. Be sure to download applications only from trusted sources.[xxxviii]
- Do not post messages, information, photos or videos of yourself if you are not sure how they will be used by an unauthorized party.[xxxix]
- Do not engage in chats or messaging with unfamiliar persons.[xl]
- Do not respond to suspicious ads, notifications or messages and delete them without opening them.[xli]

CONCLUSION

If the networking user's women follows the above preventions, they could be safe yourself from cyber crime. But if any one getting harassed online or became victim of cyber crime. Approach the police or cyber cell. Today cyber crime crossed the boundary of countries, so we need to establish a Computer Crime Research and Development Centre, Universalization of Cyber Law, Special Cyber Crime Investigation Cell for Hi-Tech Crimes , Special Cyber Courts, Regulation of Social Networking Sites, Need for Increased Awareness among Victims of Cyber Crimes, Need for Imparting Training to Officials to Investigate Cyber Crimes, Need for connecting Cyber Cafes with Police Control Rooms, Need for Development of Anti-hijacking Software and increase Education and Awareness related to Computer and Cyber-crime[xlii].

Never tell people more than what they need to know!

References-

[i]https://www.researchgate.net/publication/272478685_Social_Media_Analysis_of_New_Challenges_and_Opportunities_for_Indian_Law_Enforcement_Agencies.

[ii]https://redteamacademy.com/cyber-violence-against-women/

[iii] Agarwal Nidhi & DrNeeraj Kasuhik,(2014),' Cyber Crimes Against Women',GJRIM VO L. 4 , NO. 1 page.38-49,available on, 1 page.38-49,available on, http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC8yMjE3LnBkZnwvMjIxNy5wZGY=

[iv] https://www.techopedia.com/definition/2387/cybercrime.

[v] Barman, Nikita;(2015); 'Legal Implications of Cyber Crimes on Social Networking Websites' International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015, 315 ISSN 2250-3153, page- 316-323.

[vi] https://www.hindustantimes.com/india-news/every-sixth-cybercrime-in-india-committed-through-social-media-nia/story-KscgnwjcTZ0pzVeVaOiN6M.html.

[vii] https://www.soravjain.com/cyber-security-for-women-in-social-media.

[viii] *Ibid.*

[ix] http://cyberlaws.net/cyberindia/2CYBER27.htm

[x] Mukut (2012) "Cyber Stalking - A "Virtual" Crime With Real Consequences" available on http://worldpulse.com/node/61115

[xi] Agarwal Nidhi & Dr Neeraj Kasuhik, (2014), Cyber Crimes Against Women ,GJRIM VO L. 4 , NO. 1 page.38 available on, http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC8yMjE3LnBkZnwvMjIxNy5wZGY=

[xii] DPS Girl having fun". A complaint was made to the website owner and after 2 days of the complaint the website wrote to the seller that the content has been removed due to the violation of user agreement."

[xiii] *Ibid.*

[xiv] https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html

[xv] http://en.wikipedia.org/wiki/DPS_MMS_Scandal

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

[xvii] http://zeenews.india.com/news/nation/porn-mmses-from-delhi-metro-cctv-footage_860933.html

[xviii] Barman, Nikita;(2015); ' Legal Implications of Cyber Crimes on Social Networking Websites' International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015, 315 ISSN 2250-3153, page- 316-323.

[xix] AbhimanyuBehera, " Cyber Crimes and Law In India," XXXI,IJCC 19 (2010)

[xx] http://www.indiaforensic.com/cyberextortion.htm

[xxi] Jeet, S (2012) "Cyber crimes against women in India: Information Technology Act, 2000" Elixir International Journal Elixir Criminal Law 47 (2012) 8891-8895 available on http://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf

[xxii] Agarwal Nidhi & Dr Neeraj Kasuhik, (2014), Cyber Crimes Against Women ,GJRIM VO L. 4 , NO. 1 page.38 available on, http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC8yMjE3LnBkZnwvMjIxNy5wZGY=

[xxiii] Didwania, P (2013) "India: Cyber Defamation In Corporate World" available on http://www.mondaq.com/india/x/218890/Social+Media/Cyber+Defamation+In+Corporate+World

[xxiv] Agarwal Nidhi & Dr Neeraj Kasuhik, (2014), Cyber Crimes Against Women ,GJRIM VO L. 4 , NO. 1 page.38 available on, http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC8yMjE3LnBkZnwvMjIxNy5wZGY=

[xxv] http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf Source: Book on "IT" Security of IIBF Published by M/s Tax Mann Publishers

[xxvi] *Ibid*

[xxvii] National Cyber Security Policy -2013

[xxviii] https://www.soravjain.com/cyber-security-for-women-in-social-media.

[xxix] *Ibid.*

[xxx] *Ibid.*

[xxxi] *Ibid.*

[xxxii] *Ibid.*

[xxxiii] *Ibid.*

[xxxiv] *Ibid.*

[xxxv] https://www.civilserviceindia.com/current-affairs/articles/types-and-prevention-of-cyber-crime.html

[xxxvi] *Ibid.*

[xxxvii] *Ibid.*

[xxxviii]https://www.myadvo.in/blog/cyber-crime-in-india/

[xxxix] *Ibid.*

[xl] *Ibid.*

[xli] *Ibid.*

[xlii] Prevention and Control of Cyber Crimes in India: Problems, Issues and Strategies,http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/19/19_summary.pdf.