International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 08, 2020
ISSN: 1475-7192

THE EPIDEMIC ATTACK AGAINST WOMEN IN CYBER INFORMATION IN INDIA- A LEGAL DISSECTION

[1]K. Sofiya ,[2]A.Vedha Valli

***ABSTRACT**--Cyber violence is a great threat against the well being of an individual or group physically and mentally. Globally cyber violence is undoubtedly the new emerging form of violence and a most severe issue challenging women's dignity, security and privacy. In country like India, it is a serious threat to women where cloud technology facilities are widespread but legal awareness is low. In India, according to NCRB report violence against women in online platform is increasing rapidly every single year. The main pitfall in cyber crime is the anonimity of the criminal. The main challenge in cyber crime is tracking the criminal and deciding the governing law since cyber space is boarderless. Most of the time these crimes goes unreported. This papers presents the different form of cloud based offence against women such as cyber stalking, cyber bullying, pornography etc. This paper also discuss about the International and National legal frameworks to tackle cyber violence against women and about the lack of implementation of laws.*

***Keywords**--Cyber violence, cyber stalking, cyber bullying, pornography, social networking sites.*

I. INTRODUCTION

Cyber technology is being utilised in almost all walks of life. Almost every menage has access to internet. Cyber violence is a menace to the well-being of an individual or a group of people both physically and mentally. On a global perspective, cyber violence is a huge hazard to the dignity, security and privacy of humans, especially women. In a country like India where legal awarness is impaired, women are more vulnerable to cyber attacks. A recent study found that 40% of adult internet users have encountered online harassement, young women in particular were severly victimised.

Various modern technologies are being involved in commiting these brutal crimes. With nearly 2 billion internet users globally, more than one million women and 370,000 men are stalked annually in the United States alone. Majority of these victims are females between the age group of 18-29 years. According to National Crime Report Bereau (NCRB), cyber crime in india reached its pinnacle in the year 2017. Around 4242 cyber crime cases against women was registered out of which 1,460 online sexual harassment cases were recorded. Number of sexual harassment cases raised to 2030 in 2018 with most number of cases being recorded in Maharashtra.

In this digital era many women and men are making a career out of internet by working as a youtubers, vloggers, bloggers, instagram influencers etc which is a lucrative career. Being an online influencers they themselves posts

[1] *Assistant Professor, School of Law, Sathyabama Institute of Science and Technology, sofiyareenaadvocate@gmail.com*

[2] *Advocate, High Court of Madras, adv.vedha93@gmail.com*

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

their personal informations which makes them an easy target. Though both the genders are being victimised , female victims out number male victims. More than 75% of the victims are female.

II. COMMON FORMS OF CYBER CRIME AGAINST WOMEN

Different forms of cloud based offence against Women:

2.1 CYBER STALKING

the term "stalking" generally means to pursue or approach, prey surreptitiously. Cyber stalking involves usage of internet to stalk someone. Though the term "stalking" has been defined and punishment for the same is provided under Indian Penal Code ,there is no actual definition for the term "cyber stalking". Even Information Technology Act 2000 is silent on the definition. Cyber stalking or technology aided stalking is a novel concept which emerged as the result technological development. In cyber stalking of women, the stalker follows the victim all over the social media platform, e-mail, chats etc. There are instances wherein cyber stalking has led to henious crimes such as rapes, acid attacks , murder and robberies. Since cyber stalking is of recent origin there is lack of expertise in this field.

In 2016 National Crime Records Bureau (NCRB) reported that Hyderabad has most reported cases on cyber stalking which makes it the stalking capital in south India. In 2017 555 cases of cyber stalking has been registered in india.

In case of cyber stalking there are two scenarios in which stalking begins through internet and continues online or the stalker manages to track personal data of the victim and stalk offline.

Stalkers are of three types.

1. Obsessional stalkers: These stalkers are obsessed over sexually harrassing the victim.
2. Delusional stalkers: These talkers wants to dominate the victim which makes him feel strong.
3. Vengeful stalkers: These stalkers avenge the victim for a previous incident.

Cyber stalking involves

- harassing the victim through online chat.
- sending threating emails or texts.
- making false accusation against victim
- posting defamatory content against the victim.
- Monitoring the victim's online activities and offline locations through Global Positioning System.
- Morphing victim's photograph and blackmailing her for monetory and sexual benefits.
- Uploading the morphed pictures of the victim in porn sites.
- Identity theft.
- Accessing or destructing the data stored in victim's system.
- Sending a malware to victim's system.

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

2.2 CYBER BULLYING

Cyber bullying is when the criminals uses information technology to embarrass or humiliate or threaten the victim. The basic idea is to cause harm to the reputation of the victim. Majority of the victims are female under the age of 18. Cyber bullying involves abusing the victim in chat groups or posting defamative information or obscene pictures of the victim or posting rude comments or rumours about the victim. A recent study conducted by Child Rights and You (CRY) a NGO in 2019, with 630 adolescents, revealed that 9.2 percentage of them were victims of cyber bullying and majority of them never reported the incidents to their elders.

Furthermore the research also found out that cyber bullying of women and children has increased by 36 percentage from 2017 to 2018. But many cases goes unreported which results in underreporting of the crime.

2.3 ONLINE PORNOGRAPHY

pornography was very much in existence even in ancient times through paintings, statue, rock art etc. pornography literally means presenting a sexual act through papers or films etc to cause sexual stimulation. India is the 3rd porn watching country in the world, as a result of which pornography has become a lucrative business. Many women fall victim of a new phenomenon called “revenge porn” wherein obscene pictures of a victim are posted online without her consent. Often this is done by the victim’s ex partners. Many nonconsensual sex videos are filmed by raping the victim. These film makers get economic benefits through such pornographies. These criminals even set up a hidden camera in restrooms or changing rooms in shops or hostels etc and capture women in obscene positions and these photographs or videos are linked to porn sites. The criminals also morph the pictures of the victim and post it in porn sites with their personal details.

There are cases in which victims has taken their own lives. One such example is 2016 vinupriya’s case. A college student from salem has committed suicide after seeing her morphed semi-nude pictures in facebook. Her pictures were posted twice by the accused.

2.4 CYBER DEFAMATION

Cyber defamation is causing harm to the reputation of a person through information technology by posting false information. A large number of cases are frequently reported where cyber criminals harrass women by morphing their pictures and create obscene content of the women and post their personal information on the internet. These information are linked to pornographic websites and other social networks as a result of which women get harrassed by perverts. Social networking sites often fails to control such instances even after numerous reports.

2.5 VIOLATION OF PRIVACY

Privacy is recognised as basic human rights by UDHR and Supreme Court of India recognised privacy as a fundamental rights in Kharak singh v. state of Uttar Pradesh in 1964 and in 2017 it was reiterated in K.S.Puttasamy v. Union of India. Through gaining illegal access to a system by hacking it, the criminals mines the information about the victim. They get access to personal photographs, contact details of the victim. Even companies gain access to an induvidual’s browsing data for marketing purposes. We all might have noticed that an ad popping in our screens always matches our intrest. This is because our online search activities are being watched which is

invasion of privacy. In many instances it is reported that social networks such as Facebook leaks its users personal informations. Almost every induividuals use smart phones in which we install messaging applications such as whatsapp or messenger etc which seeks permission to access our personal data. Without allowing them to access, we cannot download the application. Here voluntarily we are permiting the applications to intrude into our privacy.

2.6 E-MAIL SPOOFING

E-mail spoofing is a most common form of cyber crime. It is a forgery of an email header which makes the reciever thinks that the email has been sent by a known person or a familiar group. These mail contains malicious wares which can access or destroy the victim's data. Email spoofing is mostly done for financial bebefits. Email spoofing is taking place through Simple Mail Transfer Protocol server as there is no mechanism for addressing authentication.

III. SCAMS OF ONLINE DATING

Online dating scammers are on constant lookout for lonely singletons. They are considered as easy targets by the criminals. Dating websites are a blessing for these criminals. In many instances these online dating has led to rapes. Women fall easy prey to these crimes and are lured into a vicious web wherein they fall for criminals and give them all their personal information. These scammers gains sexual and monetary benefit from victims. A research conducted on a group of 72 women regarding cyber stalking in female students states that 12.5 percentage of the victim had physical intercouse with the criminals before being stalked. And in majority of the cases the crime started through online chats. There are plethora of matrimonial sites in our country wherein parents themselves create a profile for their sons and daughters and giving out all the personal data.

Let us not forget the burning pollachi issue 2019 where in victims met their predators online and created virtual friendship with them which led to sextortion. This henious crime,which was prevailing for a longer period of time, came into light only when a victim came forward to report the violence. FIR was filed against four accused under section 354A and B and 394 of IPC and section 66E of IT act. Number of videos has been confiscated by the authority involving many other victims. It is important to note that none other victims came forward to report the case as a fear of getting exposed. Especially in a society where women are criticized and blamed for even getting raped. Criminals take leverage of this fear and victimise women both online and offline.

IV. SOME OF THE REPORTED INSTANCES

4.1. RITU KHOLI CASE- India's first cyber stalking case.

In this case Mrs Ritu Kholi filed a complaint against one, Manish Kathuria before the Delhi police deparetment as she was being stalked by him over the internet at the website www.mirc.com, for four consecutive days. Furthermore the accused also used her identity to chat with others in her name and posted her contact details online along with filthy language. Mrs.Kohli received about 40 obnoxious calls in the span of 3 days from places like Kuwait, Cochin, Bombay and Ahmedabad. Delhi police traced the IP addresses to a Manish Kathuria. He pleaded guilty and was arrested under section 509 of the IPC nothing in the IT Act.

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

4.2. In State of Tamilnadu v. Dr.L.Prakash 2002, the accused is a surgeon. He captured obscene pictures of his female patients and circulated the same in the internet. He was given lif sentence along with three of his staffs.

4.3. In 2012, South Indian singer Chinmayee filed a complaint before Chennai Police Commissioner as she and her mother was being abused and threatened by someone via twitter and facebook. The accused was then arrested under IT Act 2000 and Tamil Nadu Prohibition of Women Harassment Act

4.4. In Karan Girotra v. State, the complainant Shivani Saxena who was a divorcee met Karan Girotra online who promised to marry her. Karan invited Saxena over and he drugged her and sexually assaulted her. He made obscene photographs of the victim and later blackmailed her with the photographs. But in this case judiciary favored the accused and stated that Saxena gave consent to sexual intercourse and she delayed in filing an FIR gainst accused. She only filed the complaint when he denied to marry her.

4.5 State of Tamilnadu v. Suhas katti 2004, is the first ever case in which the accused is convicted under section 67 of IT Act. Since the victim denied to marry the accused he started stalking her and harrasing her online. He was held guilty under section 469 and 509 of IPC and section 67 of IT act and he was sentenced for rigourous imprisonment of two years with fine.

V. INTERNATIONAL AND NATIONAL LEGAL FRAMEWORKS ON CYBER CRIME AGAINST WOMEN.

It is important to note that though we have few International conventions on cybercrime , none of the conventions are established especially to deal with violence gainst women.

5.1.INTERNATIONAL FRAMEWORK

5.1.1 EU CONVENTION ON CYBER CRIME 2001.(Budapest Convention)

The convention which was signed at Budapest is the first and most significant International instrument to deal with internet and cyber crime. It was drawn by European Council. The main objective of Budapest Convention is to harmonise National laws, improving investigative techniques and increasing cooperation among Nations. At present it is the only existing treaty under United Nations on cyber crime. Only under this convention many offences are recognised as cyber crime. Though India is not a signatory to this convention, some of the provisions in our IT Act is inspired by the convention.

5.1.2. CONVENTION ON ELIMINATION OF ALL FORMS OF DISCRIMINATION AGAINST WOMEN(CEDAW)

Article 6 of CEDAW convention urges States Parties to take all appropriate measures, including legislation, to control all forms of trafficking against women and exploitation of women through prostitution.

5.1.3 BEIJING DECLARATION OF WOMEN'S RIGHTS

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.

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

5.1.4 The United Nation on December 27th 2019, approved a new resolution in order to draft an International treaty to combat cybercrime. The draft resolution was prepared by Russia and approved by 193 member countries. The draft proposes to establish an expert committee.

5.2. NATIONAL FRAMEWORK

5.2.1. INDIAN PENAL CODE

- Section 292 prohibits sale, distribution, publication, advertising, importing, exporting, hiriring,production of any obscene content. Though the section does not expressely mention about online obscenity, by applying mischeif rule of interpretation the terms " any other object" implies that any obscene content in any form is included under the section. Section 292 also provides for exceptions in which the section is not extended to any material which is used for art, science, literature, religious purpose or in any ancient monuments within the meaning of the Ancient Monuments and Archaeological Sites and Remains Act 1958.
- Section 293 prohibits the sales of Obscene objects to young person.
- Section 294 prohibits any obscene acts in the public.

It is to be noted that IPC does not define the term "obscene" . The concept of obscenity differs from place to place.

India recorded the highest ratio in the world for spam or junk mail. In India pc owners are the most targeted sector of cyber-attacks. Mumbai and Delhi has been recorded as the top two cities for cybercrime.

- Section 354C Prohibits voyeurism. Watching or capturing and disseminating any sexual activity of a women is a punishable offence.
- Section 354D prohibits stalking of women repeatedly despite a clear indication of her disinterest. The section expressely covers stalking by electronic communication and internet.
- Section 469 prohits forgery of electronic document to harm the reputaion of a person.
- Section 499 prohibits defamation of living or deceased person.
- Section 507 prohibits criminal intimidation by an unonymous communication.
- Section 509 prohibits uttering any a word or making gesture or sound to insult a women's modesty.

5.2.2 INFORMATION TECHNOLOGY ACT 2000

- Section 66A which provided for punishment for sending offensive messages through communication services was struck down by Supreme Court in Shreya Shingal v. Union Of India in 2015.
- Section 66C provides for punishment for identity theft.
- Section 66D provides for punishment for cheating by personation by using computer resources.
- Section 66E provides punishment for violation of privacy.
- Section 67 provides punishment for publishing or transmitting obscene material in electronic form.
- Section 67A provides punishment for publishing or transmitting of material containing sexually explicit act in electronic form.
- Section 67B provides punishment for publishing or transmitting of child pornography.

It is to be noted that these provisions of IT act is not specifically enacted to deal with female victim.

5.2.3. INDECENT REPRESENTATION OF WOMEN (PROHIBITION) ACT 1986.

- Section 4 prohibits publication or sending by post of any material which contains indecent representation of women in any form.
- Amendment bill of 2012 seeks to widen the scope of the act and include internet or any other e-form.

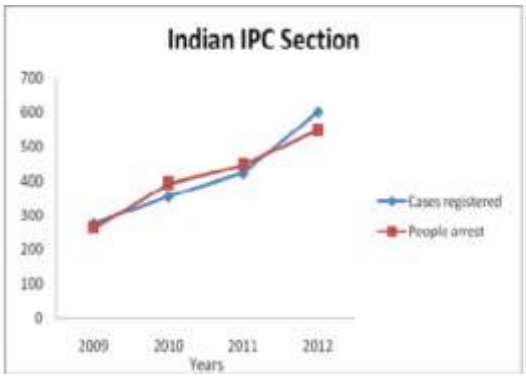

Fig.3. Case registered under Indian IPC section

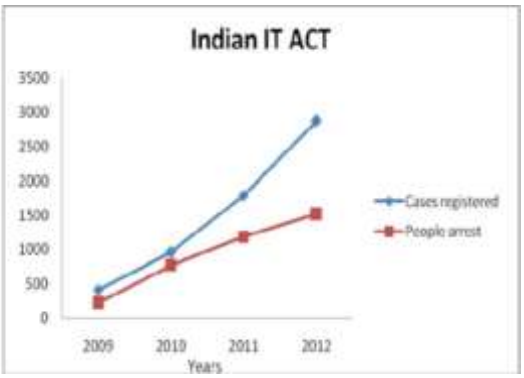

Fig.4. Case registered under Indian IT Act

(Source: Crime in India- 2012, Compendium, National Crime Records Bureau Ministry of Home Affairs Government of India)

VI. CONCLUSION

Though both genders are being victimized by cyber criminals, women in particular suffers more. This is due to the stereotypes that we have in our society. Women are seen as a sex objects by these criminals. Men seldom faces sexual abuse. Easy availability of personal data is a boon for cyber criminals. Victims have partial understanding about how the cyber world functions. Though they have knowledge about technology, they often fail to see the pitfalls of the technology. Often these victims are new to cyber space and they are inexperienced. Though Indian Penal Code and Information Technology Act provides for punishing cyber criminals, identitifying the criminal is a great challenge since internet is a global phenomenon and often these criminals stay anonymous. Law enforcement agencies have to realize the gravity of the situation and frame a comprehensive law or enhance the existing law for tackling violence against women in cyber world. Lack of clarity in our existing law and empirical study in this field is a major drawback. Statistics that are available right now are not exact numbers as many instances of cyber crime against women goes unreported. In 2019 Union Home Ministry had published a booklet titled " A handbook for students on cyber safety" which provides safety guidelines against cyber crime. Such other awarness measures should be taken by the Government and it should be included in curriculum of the students.

REFERENCES

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

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

2. http://www.legalserviceindia.com/article/l146-Cyber-Crime-And-Law.html
3. http://shodhganga.inflibnet.ac.in/bitstream/10603/130487/9/09_chapter%204.pdf
4. https://www.researchgate.net/publication/262388740_Latest_Face_of_Cybercrime_and_Its_Prevention_In_India
5. http://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf
6. http://www.ijcrt.org/papers/IJCRT1807078.pdf
7. file:///C:/Users/user/Downloads/SSRN-id2486125.pdf
8. https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf
9. General Assembly resolution 55/25 of 15 November 2000
10. https://indiankanoon.org/doc/170577355/ retrieved on 02/10/2016
11. http://www.un.org/womenwatch/daw/cedaw/ retrieved on 02/10/2016

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020