CHAPTER-14

LAW ON CYBER CRIME AND STUDY ON ITS LEGAL FRAME WORK

[1]Ms. NABA JAHAN, [2]Mr. NAZIM ALI KHAN

[1]Assistant Professor, Department of Law, Harsaun Enclave, Govindpuram Ghaziabad

[2]Architect, Harsaun Enclave, Govindpuram Ghaziabad

Chapter ID: NSP/ICAAR-2023/A-14

ABSTRACT

In Cyber Crime , private information of an individual is extract that can be directly or indirectly which involves mainly activities that use internet with the help of computer system by using that private information Illegally without the consent of person's with the motive of humiliating the reputation or harming the person mentally or physically with the advancement in technology a steep increase in the rate of Cyber Crimes has been notices with the advancement in technology most of the world is depending on the internet, with the increase of dependency on cyberspace internet crimes committed against women have also increased. This increase in the increase of cybercrime can be cause many internets user don't know about the functioning of online platforms; they avoid technological advancements and have minimal adequate training and education. Hence, Cyber Crime has emerged as a major threat for the enforcement agencies of different countries for the protection of different countries for the protection of women and children who are molested, harassed and abused for their curious and voyeuristic pleasures. India is the country where IT Act is followed to deal with issues pertaining to Cyber Crimes in order to protect all the person from exploitation.

Keywords: *Cyber Crime, IT Act, Internet, Technology, Women.*

INTRODUCTION

The advent of technology has provided women an opportunity to explore their strengths and widen their capabilities. With the rapid modernisation taking place all over the world, internet has become a part of our daily lives. It has proved to be an efficient tool of communication. However, with the increase of dependency on cyberspace internet crimes committed against women have also increased. Women all over the world have been victims to a number of harassments for decades now. With the advent of technology and digitalisation people have the ability to communicate virtually with anybody, anytime and anywhere across the globe. Cyber-crime has emerged as one of the results of this modernisation. Online platforms are often used to harass and abuse women for voyeuristic pleasures. One of the major reasons as to why it takes place is because of the fact that around more than half of the online users are not fully aware of the functioning of online platforms such as WhatsApp, skype, Facebook, etc. Women are commonly targeted for cyber stalking, cyber pornography, impersonation etc. The victims often trust the offender and share their private data or information as a consequence of which innumerable cyber-crimes take place daily.Cyber-crime has become a concept wherein majority of cases the victims have been women who have fallen prey to technological fancies. A steep increase in the rate of cyber-crimes has been observed in different countries where the primary concern has always been the protection of women. India is one of the few countries which has enacted the IT Act 2000 to deal with

issues pertaining to cyber-crimes in order to protect the women from exploitation by vicious predators and provide them support so that they can fight back against all wrongdoings.

WHAT IS CYBER CRIME?

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones"

Cyber-crime involves the use of internet and computer. It threatens an individual's privacy by disclosing or publishing their personal or confidential information online with the aim of degrading their reputation and causing them physical or mental harm either directly or indirectly. Women are generally the targets of these offenders because they are inexperienced and lack knowledge of the cyber world, thereby falling prey to the technological fancies.

Types of Cyber Crime

Cyberstalking: In today's modern world, it is one of the most commonly committed crimes. It involves following a person's movements and pursuing him/her stealthily. It involves gathering data that maybe used to harass a person or making false accusations or threats. A cyber stalker uses internet to stalk someone and thus, doesn't pose a direct physical threat to an individual but due to the anonymity of the interactions that take place online the chances of identification of the cyber stalker becomes quite difficult which makes this crime more common than physical stalking.

Cyber Pornography: It is a major threat to women and children security as it involves publishing and transmitting pornographic pictures, photos or writings using the internet which can be reproduced on various other electronic devices instantly. It refers to portrayal of sexual material on the internet.

According to IT Amendment Act 2008 "crime of pornography under section 67-A, whoever publishes and transmits or causes to be a published and transmitted in the electronic form any material which contains sexually explicit act or conduct can be called as pornography. Section 292/293/294, 500/506 and 509 of Indian Panel Code, 1860

Cyber Morphing: It is a form of crime in which the original picture is edited by an unauthorised user or a person possessing a fake identity. Photographs are taken of female users from their profiles and are then reposted for pornographic purposes by fake accounts on different sites after editing them. Due to the lack of awareness among the users the criminals are encouraged to commit such heinous crimes. Cyber morphing or Cyber obscenity is punishable under section 43 and 66 of Information Act 2000.

Cyber Bullying: Cyberbullying involves the use of internet for causing embarrassment or humiliation to someone place by sharing their personal or private data by sending, posting or sharing harmful or false content over digital devices like computers, tablets, laptops and cell phones. It can take place through SMS, online gaming communities, online forums or social media platforms wherein information can be exchanged online and is available to a number of people. Cyberbullying is persistent and permanent and therefore, can harm the online reputation of not just the victim but both the parties involved.

Email Spoofing and Impersonation: It is one of the most common cybercrimes. It involves sending e-mail which represents its origin. Email spoofing is mostly used to extract personal information and private images from women fraudulently and are later used to blackmail them. According to a report, there has been a 280% of increase of phishing attacks since 2016.

Email spoofing is an offence under section 66-D of the Information Technology Amendment Act, 2008 and section 417, 419 and 465 of Indian Panel Code 1860

Online Trolling: It is a form of online violence on social media platforms where people are given the liberty to speak their mind. Online harassers often tend to target people who express their opinions and think differently from the prevailing societal norms. On such section constitutes of females who are targeted by social media bullies. According to Digital Himayat report, "women that are vocal online, especially on topics that have been traditionally relegated to 'male expertise' like religion or politics, or about women's experiences, including those of sexuality, menstruation, or speaking out about patriarchy, are subjected to a vicious form of trolling, usually from self-identified right-wing accounts on Twitter."

EXTENT OF CYBERCRIME AGAINST WOMEN IN INDIA

With approximately 688 million active users, India is the second largest internet market in the world.[5] Sites like Facebook, YouTube, Twitter, Instagram, WhatsApp and Snapchat are the most liked in India. While internet population has been increasing there still is a gender divide. According to a report published by IAMAI (Internet and Mobile Association of India) on internet usage in India, about 67% of the users are male compared to which only 33% are female.

One of the major reasons for the rise of cyber-crime against women apart from the advancement of internet is the fact that Indian women are not open on reporting a cyber-crime. They fear that it will bring disgrace to their families. Most of the times they believe that it is their own fault that the crime happened. Cyber space is a world on its own and people come and go as they please. This makes the cyber criminals to commit a crime and escape punishment easily. Through various instances it can be seen that women befriend men on the internet who forms a bond by discussing their lives and pretending to be the woman's true friend. Gradually they form a strong friendship and then starts to send obscene messages. A 2016 survey on Violence Online in India conducted by the Feminism in India portal on 500 individuals (97% women and 3% trans-genders) found that 58 percent of respondents "had faced some kind of online aggression in the form of trolling, bullying, abuse or harassment". But 38% of those who faced such violence did not take any action

THE LEGAL FRAMEWORK

There are two unique features of the Internet. Firstly, it is not confined to a particular boundary and the cyber-criminal can commit a crime from ay part of the world. The second unique feature is that it provides anonymity to its users which has its own boon and bane There are many laws in statues and regulations which penalises cyber-crime. But the majority of the laws belong to the Indian penal Code (IPC), 1860 and the Information technology Act (IT Act), 2000. The IPC is the general criminal code of India which defines offences and prescribes punishment for the same. IPC covers laws and punishment pertaining to physical world and has been legislatively amended and judiciously interpreted to be applicable to cyber criminals. Whereas the IT Act is a specific code pertaining to use of information technology and crime committed through it. In 2008 IT Amendment Act was enacted inclusive of certain crimes related to cyber world.

What forms of online VAW can this provision help in challenging?

IT Act Section 66E: The capture and electronic transmission of images of private parts of a person, without his/her consent.–

Section 67: The publishing or transmission of obscene material in electronic form– Graphic sexual abuse on social media and blog platforms, including trolling.

Section 67A: The publishing or transmission of sexually explicit content in electronic form.

Section 67B: The electronic publishing or transmission of material in electronic form that depicts children in obscene or indecent or sexually explicit manner.

IPCSection 354 ASexual harassment, including by showing pornography against the will of a woman

Section 354 C: Voyeurism, including watching or capturing the image of a woman engaging in a private act in circumstances where she would have a reasonable expectation of not being observed; and dissemination of images of a woman engaging in a private act under circumstances where she has agree to the capture of images but not to their dissemination.

Section 354D: Following a woman, contacting/ attempting to contact her to foster personal interaction repeatedly despite a clear indication of disinterest by such woman, or monitoring the use by a woman of the Internet, email, or any other form of electronic communication – Cyber-stalking.

Section 499: Criminal Defamation that leads to reputational harm

Section 507: Criminal intimidation by anonymous communication.

SUGGESTIONS

While using online platform not divulging any personal data is almost impossible and thus, one should beware while sharing any personal information online. It is imperative that an eye should be kept on phony email messages and such emails should not be responded to that ask for personal information. Also, email address should be guarded. While engaging in online activities it is imperative that attention should be paid to privacy policies on websites and steer clear of fraudulent websites used to steal personal information. It is necessary that response to offences on the internet against women should be seen as part of the broader movement against harassment and abuse. Broader efforts should be initiated as it is ultimately a people- centred challenge. Keeping up with the pace of change is the need of the hour. Keeping up with the technological advancements is a challenge that is essential to overcome as most of the online crimes takes place due to the lack of knowledge and awareness among the users.

A collaborative effort among media, clubs, associations and women's media networks is critical to promote women's leadership and decision making in the society. Online diligence, monitoring and reporting against violence and cyber-crime should be done effectively and efficiently. Women should be made aware about using online media platforms and adequate procedures should be followed by them. They need to be aware of their right in the cyberspace. The government should make more rigid rules to apply on the Internet Service Providers (ISPs) as they have the entire record of the data that is accuses by the users surfing on the web. Also, in case of any suspicious activities a report should be made by them in order to prevent crimes at an early stage.

CONCLUSION

"The law is not the be-all and end-all solution." Victims are still not getting justice despite of a strong legal base in spite of them remaining silent. Cyber-crime against women is just a reality check of what really is going on in the real world. The lines between the online and offline world is getting blurred. Cyber-crime happens because the criminals think that is a much easier way with less punishment. With millions of users in the online platform's complaint mechanisms has also become fruitless. For instance,

in the recent boy's locker room case where group of teenage boys from Delhi shared pictures of underage women and objectified them by passing derogatory comments on group chat in Instagram and Snapchat. When a girl shared the screenshots of the chats the group was busted. Women all over country raised voices but it could be seen that they were not shocked. The reason is that objectification of women has become quite normal in the society. Women have had accepted this mentality of objectification by male as every day new cases come into light. Years have passed and still women live in the fear of going out alone outside in the real world. In fact, the online world which she could go to in the safety of her home has also become an unsafe place. It comes upon the women to take preventive measures such as usage of data security, not leaving digital footprint, keeping everything password protected. But this are all superficial ways. The major problem that has always been existing is the patriarchy and misogyny in the society. To solve this problem a long-termmeasure, need to be undertaken that will help in dealing with cyber-crime against women. There is the need of the hour to evolve the societal and cultural norms with the development of information technology. Mandatory steps need to be taken. Steps like digital literacy, development of data security, providing access of technology to women and girls and most of all enactment of laws specifically on cyber-crime especially with reference to women.

REFERENCES

1. *DEBRATI HALDER & K.JAISHANKAR, CYBER CRIMES AGAINST WOMEN IN INDIA*
2. *Adv. Prashant Mali, IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1.*
3. *Case of Cyber Extortion, INDIA FORENSIC, (Jan 20, 2021), http://www.indiaforensic.com/cyberextortion.htm*
4. *Trolls Target Women: Dealing with Online Violence, THE CITIZEN, (Jan 21, 2021), https://www.thecitizen.in/ index.php/en/NewsDetail/index/7/17330/Trolls-Target-Women-Dealing-with-Online-Violence*
5. *Digital population in India as of January 2020, STATISTA, (Jan 21, 2021), www.statista.com/statistics/309866/India-digital-population/.*
6. *India Internet 2019, IAMAI, (Jan 28, 2021), https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf*
7. *Crime in India- 2018, NCRB, (Jan 28, 2021), https://ncrb.gov.in/crime-india-20*
8. *Pasricha &Jasleen, "Violence" online in India: Cybercrimes against women and minorities on social media, http://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf*
9. *Technology-mediated violence against women in India, IT FOR CHANGE, (Jan 29, 2021), https://itforchange.net/e-vaw/wp-content/uploads/2017/12/DISCUSSIONPAPER.pdf*
10. *"Information privacy, or data privacy (or data protection), concerns personally identifiable information or other sensitive information and how it is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. In relation to technology, it pertains to the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them."*
11. *Supra note 9*
12. *Breach of privacy and confidentiality*
13. *Data Theft*