INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 2

2021

A Study on Cyber Crime and its Legal Framework in India

APOORVA BHANGLA[1] AND JAHANVI TULI[2]

ABSTRACT

Cyber-crime mainly involves activities that use internet and computers as a tool to extract private information of an individual either directly or indirectly and disclosing it on online platforms without the person's consent or illegally with the aim of degrading the reputation or causing mental or physical harm. With the advancement in technology a steep increase in the rate of cyber-crimes has been observed. With the increase of dependency on cyberspace internet crimes committed against women have also increased. This is mainly because around more than half of the online users are not fully aware of the functioning of online platforms, they are ignorant towards technological advancements and have minimal adequate training and education. Thus, cybercrime has emerged as a major challenge for the law enforcement agencies of different countries in order to protect women and children who are harassed and abused for voyeuristic pleasures. Women are commonly targeted for cyber stalking, cyber pornography, impersonation etc. 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 however this act doesn't address some of the gravest dangers to the security of the women and issues involving women are still growing immensely.

Keywords: *Cyber-crime, women, IT Act, technology, online platforms.*

I. 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-

[1] Author is a Student at NMIMS School of Law, India.
[2] Author is a Student at NMIMS School of Law, India.

 [ISSN 2581-5369]

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. There is minimal adequate training and education that is provided to the users. Moreover, ignorance towards technological advancements has carved its way for such heinous crimes. 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. Due to fear of defamation in the society and lack of evidence it becomes really difficult to identify the origin of the crime. 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. Many institutions have taken up the issues pertaining to cybercrime in order to raise awareness for the safety of women but still a steep increase has been observed in this area, which poses a negative impact on the development of the nation.

II. 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".[3]

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.

Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined "cybercrime against women" as "Crimes targeted against women with a motive to

[3] DEBRATI HALDER & K. JAISHANKAR, CYBER CRIMES AGAINST WOMEN IN INDIA

 [ISSN 2581-5369]

intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".

TYPES OF CYBER CRIME

1. 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.

One of the major targets of cyber stalking is women and children who are stalked by men and adult predators namely, for revenge, for sexual harassment and for ego. Most of the times, the victim is unaware of the use and rules of the internet and the anonymity of the users has contributed to the rise of cyber stalking as a form of crime. The offender for committing this offence maybe charged for breach of confidentiality and privacy under section 72 of the IT Act, 2000 as cyber stalking is yet not covered under existing cyber laws in India. Also, section 441 and 509 of IPC are also applicable for the same.

2. 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 A.P. Mali, "It is the graphic, sexually explicit subordination of women through pictures or words that also includes pornography is verbal or pictorial material which represents or describes sexual behaviour that is degrading or abusive to one or more of participants in such a way as to endorse the degradation. The person has chosen or consented to be harmed, abused, subjected to coercion does not alter the degrading character of such behaviour." [4]Around 50% of the total websites on the internet show pornographic material wherein photos and pictures of women are posted online that are dangerous to women's integrity.

[4] Adv. Prashant Mali, *IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1*.

 [ISSN 2581-5369]

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 are also applicable and victim can file a complaint near the Police Station where the crime has been committed or where he comes to know about crime. After proving crime, the accused can be called as first conviction with an imprisonment for a term which may extend to five years including fine which may extend to ten lakh rupees. In the second conviction the term of imprisonment may extend to seven years and fine may extend to ten lakh rupees".

3. 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.

4. 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.

5. Email Spoofing and Impersonation

It is one of the most common cybercrime. It involves sending e-mail which represents its origin. In today's times, this from of crime has become immensely common that it becomes really difficult to assess as to whether the mail that is received is truly from the original sender. 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. Avanan research depicts that around 4% of the total emails that are received by an individual user are fraudulent emails. In Gujarat Ambuja's Executive case, the 51 year old cyber 1 criminal created a fake email ID and pretending to be

 [ISSN 2581-5369]

a woman indulged in a "cyber relationship" extorting Rs 96 lakh from an Abu Dhabi based businessman.[5]

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. It is a cognizable, bailable and compoundable offence with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

6. 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 Hifazat 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." [6]

Social media bullying takes a toll on the mental as well as the physical health of the victims. Abuse, hate speech and mean comments are the most common elements of trolling. The most common consequences of trolling are self-censorship and mental health concerns.

III. EXTENT OF CYBERCRIME AGAINST WOMEN IN INDIA

With approximately 688 million active users, India is the second largest internet market in the world.[7] 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.[8] This disparity between the male and female users is the major reason for the growth of cybercrime incidents against women.

Cyber-crimes are illegal activities which is forbidden by the law and committed by the use of internet and cyber technology. Cyber-crimes can be committed against any person, property or

[5] *Case of Cyber Extortion*, INDIA FORENSIC, (Jan 20, 2021), http://www.indiaforensic.com/cyberextortion.htm
[6] *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
[7] *Digital population in India as of January 2020*, STATISTA, (Jan 21, 2021), www.statista.com/statistics/309866/india-digital-population/.
[8] *India Internet 2019*, IAMAI, (Jan 28, 2021), https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf

government but this paper solely focuses on cyber- crimes against women. According to National Crime Research Bureau there was sharp increase in the number of reported cyber-crime in 2017 in comparison to past years. Further increase in the reported cybercrimes can be seen in the year 2018. "While a total of 21,796 crimes were recorded under both IPC and IT Act in 2017, the number has increased to 27,248 in 2018."[9] In 2017 NCRB for the first time had included categories relating to women and child on the nature of crimes committed against them.

Since the 1990s the information technology has taken giant strides forward and every family who has a modest income has the internet service. Individuals from varying age are able to use it everywhere starting from their home to their workplace. It can be deduced that internet has become a world on its own with its own place where one can share, have cultural values or opportunities. But it has its own disadvantages, the cyber world has become a place for wrongdoers to defraud women and some even going as low as to encroach children. The ceaseless advancement of internet is making it harder to detect and regulate leading to rise of cyber criminals. Due to technological innovations cyber criminals are able to commit crime with a fake identity from any place in the world. This means that they do not have any physical contact with the real world and are mostly getting away with it without any punishment. With the protection of anonymity people are able to access any kind of material on the web which leads to huge number of anti-social, violent and aggressive content.

One of the major reason 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. In this tinstance it is the duty of the woman to report the person but it can be seen that in the most of the cases they shy away and this gives more courage to the cyber-criminal. 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

[9] *Crime in India- 2018*, NCRB, (Jan 28, 2021), https://ncrb.gov.in/crime-india-2018

 [ISSN 2581-5369]

did not take any action.[10] The victim women needs to understand that by reporting the man the problem can be solved and further saving the lives of other woman who can be the criminal's future targets.

IV. 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 provide anonymity to its users which has its own boon and bane. For people who use this anonymity for putting out their opinion to the world it's a boon but the perpetrators who use this anonymity for commission of crime it is a bane. Therefore this features not only pose a challenge in crime prevention but also in the implementation of law. At present there is no specific law that deals with cyber-crime against women. Other laws which can be used in the specific case, most women are not aware of. Women does not know about their rights or that such rights exist.

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. Both IT Act and IPC are complementary to each other on cyber-crime against women. The below mentioned table is taken from a discussion paper published by IT for Change it showcases the laws that a cyber-criminal can be charged with when he/she commits a crime against women. Following which the loopholes in the said laws is analysed.

Act	**Clause**	**Details of the offence this provision addresses**	**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,	- Non-consensual circulation and malicious distribution of sexually explicit photographic

[10] Pasricha & Japleen, *"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

		without his/her consent.	and video material about an individual.
	Section 67	The publishing or transmission of obscene material in electronic form.	- Graphic sexual abuse on social media and blog platforms, including trolling. - Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
	Section 67A	The publishing or transmission of sexually explicit content in electronic form.	- Graphic sexual abuse on social media and blog platforms, including trolling. - Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
	Section 67B	The electronic publishing or transmission of material in electronic form that depicts children in obscene or indecent or sexually explicit manner.	- Circulation of child pornography
IPC	Section 354 A	Sexual harassment, including by showing pornography against the will of a woman	- Graphic sexual abuse on social media and blog platforms, including trolling. - Sending video and pictures with sexually explicit content and images to a woman, against her will.
	Section 354 C	Voyeurism, including watching or capturing the image of a woman engaging in a private act in	- Non-consensual production, circulation and malicious distribution of sexually explicit

		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.	photographic and video material about a woman.
	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. Only women are recognized as potential victims by the law.
	Section 499	Criminal Defamation that leads to reputational harm	-Though this is a gender neutral provision, it could be invoked by women bloggers and women on social media fighting slander and libel.
	Section 507	Criminal intimidation by anonymous communication	- Though this is a gender neutral provision, it could be invoked by women fighting trolls issuing threats, whose identities are often anonymous.
	Section 509	Word, gesture, act or exhibition of an object intended to insult the modesty of a woman.	- Though this provision does not explicitly address online sexual harassment and abuse, it could be invoked in such cases.

Table 1. Key legal provisions that can be invoked to address online Violence against women[11]

[11] *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

Lacuna in the Existing Provision of Law

- The verbal abuse made online which does not contain any sexual content is not properly tackled. General sexist comments have not been taken under Section 499 and Section 507 of the IPC which deals with criminal defamation and criminal intimidation pertaining to those trolls that are of personal nature. Further, doxing without any circulation of sexual material and without any intimidation is not included. Section 66 of the IT Act criminalises hacking but it does not explicitly state the act of doxing through hacking.

Online trolling, verbal abuse, hacking for doxing has been treated as personal and isolated crime in Section 499 and Section 507 of IPC and Section 66 of the IT Act. It is important to note that this act of abuse is committed against women because she is a women. From the past it can be seen that the abuse is based on the women's sexuality and caste.

- Section 66E of IT Act and Section 354C, Section 354D of the Criminal Laws Amendment Act 2013 are the exception to violence as physical harm and not as intrusion to bodily integrity and personal autonomy as defined by the other sections of IT Act and IPC. These sections also just focuses on physical privacy and not on the "informational privacy".[12] It is to be considered that Section 509 of IPC mention "Privacy" but it only talks about privacy with respect to women's modesty. "Sexual violence is largely viewed from the standpoint of maintaining public decency through curbing obscenity and protecting the modesty of women."[13] Further, it can be seen that withdrawn at any point. Sexual violence is combined with the need to regulate the ratification and representation of sexuality which results in reinforcing genders norms of protecting women's sexuality rather than protecting her bodily integrity or their informational privacy. Section 72[14] and Section 43 read with Section 66 [15] of the IT Act is an economic offence and not a gender or social offence.

- Psychological violence based on gender against women is not recognised by the law outside their familial setting. Acknowledgement of psychological violence that is the circulation of private information through infringement of privacy which is not of sexual nature is not been done.

- Additionally laws like Protection of Women from Domestic Violence Act, 2005 which deals with cases related to psychological violence at home and live in relationships does not

[12] "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."
[13] *supra* note 9
[14] Breach of privacy and confidentiality
[15] Data Theft

talk about cybercrime with respect to women.

V. SUGGESTIONS

1. While using online platform not divulging any personal data is almost impossible and thus, one should beware while sharing any personal information online.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Online diligence, monitoring and reporting against violence and cyber-crime should be done effectively and efficiently.
8. There should be an E-portal where women can report their problems online themselves without suffering from the stigma of involving police in such matters. Also, the database of criminals should be maintained which could help in law enforcement.
9. 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.
10. Education systems must initiate contemporary issues regarding online crimes and awareness should be spread regarding safe internet uses.
11. 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.

 [ISSN 2581-5369]

VI. 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 platforms 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 has accepted this mentality of objectification by male as every day new cases come into light. Years have passed and still women lives 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 term measure 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.

*****

 [ISSN 2581-5369]