Law Journals
A Treasure Trove of Legal Knowledge

National Journal of Cyber Security Law

Volume 3, Issue 1
www.stmjournals.com

Cyber Crimes against Women: Legal Precautions the Government should Enforce in India

Pritam Mirdha[1,*], *Md. Umar Faiz*[2]
[1,2]Student, Amity Law School, Amity University, Raipur, Chhattisgarh, India

Abstract

In this modern era the crimes against women are at peak of it. The crime done against women can be in many ways, it can be physical, or it can be on internet (cyber). The crime rates are more on internet (cyber) then physically, which affects the whole family of a woman and the woman herself, and which leads to lots of miss happenings. In India the crime rate physically and on internet (cyber) has become more comparing to the earlier times. To which the government should pass and enforce strict laws and the government should stick to it.

Crimes against women in India

Crime head	Crime incidence			Crime rate		
	2014	2015	2016	2014	2015	2016
Total crime against women	3,39,457	3,29,243	3,38,954	56.6	54.6	55.2

It is a record by the National Crime Records Bureau Ministry of Home Affairs where it is been seen that the crime against women has gradually increased in subsequent years.

Cybercrimes in India

Crime head	Crime incidence			Percentage Variation	
	2014	2015	2016	2014–2015	2015–2016
Total cyber crime	9,622	11,592	12,317	20.5%	6.3%

Here is another record by National Crime Records Bureau Ministry of Home Affairs where it is seen that the cybercrimes have also increased year to year. This paper is going to deal with the cybercrimes against women and would provide Legal suggestions to stop the cybercrimes against women and will help to stop many cybercrimes overall.

Keywords: *cybercrime, women, internet, government, defamation, social media, technology, threats, victim, offence*

****Author for Correspondence*** E-mail: rssbmirdha2@gmail.com

INTRODUCTION

Cybercrime is a crime which is not done physically, it is done over internet for example- stalking, trolling, defamation, body shaming etc.

"Time is now here to exculpate that our women are safe in cyber world, the memento alarms to stop tomfoolery activities on internet access as it is an offence and women take umbrage from it" [1]. In this modern era where everyone is attached to social media (Facebook, Instagram, WhatsApp etc) through internet, which has become a great threat for the women or girl. In cybercrime against women the effect is more in mental then on physical. In India at least one woman is trapped on internet. Technology is very helpful for everyone, but it is also very harmful for everyone. There are some, remedies for this which is introduced by the government, but everyone does not know about these. Many people know about the remedies which should be done after any women has victim of cybercrime, but they don't do it as they think that what will be the effect on them after they take any action against that. And many are there who want to report but they don't know the process or the right place where to file a report. In India there is National Crime Records Bureau (NCRB) who records all the crimes happening in India, but it does not record the crime happening on internet. There are various ways in which a woman can be harmed in the

matter of reputation, and in any place of the world the reputation of a woman is given a big matter of priority, so the wrong doers send many obscene things to a woman or stalk a woman, even if their mind does not get satisfied then they do the worst of all by developing pornographic videos etc. The cybercrimes which take place are done through fake Facebook accounts, Twitter accounts, WhatsApp accounts etc which could not be understood by every person. Cybercrime can be done for many purposes such as to take revenge, to get an illegal gain, blackmailing for some purpose etc. As cybercrime does not harm anyone from outside so women and girls get sever diseases such as hypertension, blood pressure, heart diseases etc. In India girls and women should be trained if any day they are been trapped or become a victim of cybercrime then they should be able to report it to the concerned authority within time. Emerging in the 21st century, cybercrime has fast become the most severe issue challenging our security and privacy. It is serious in case of states like India where information technology facilities are widespread but legal awareness in general is low. The legal entity or the legal process of India is still unable to deal with the crimes or the violence happening in the cyber world [2].

ELEMENT WITHOUT WHICH A CRIME IS NOT A CRIME WHETHER CYBER OR NOT

The main elements are:

1. Actus reus
2. Mens rea

Actus Reus

Actus Reus means "any act or any guilty deed". Any person cannot be held liable without any guilty deed or act. A person can be made liable for any guilty act. An act can be said guilty act, if it is done against any criminal code or violation of the constitutional law of India [3].

How is Actus Reus related to Internet crimes?
In case of internet crimes, it is easy to identify the Actus reus but it is very difficult to prove. This means that you can understand that you are been trapped but you cannot know that who trapped you or from where you are being trapped.

A person can be held liable for cybercrime when:

1. Making use of any computer system for illegal purposes
2. Surfing to any unauthorised data which is saved in another system.
3. These are the main ways to commit cybercrime. The main purpose of doing cybercrime is to have an illegal gain.

Mens rea

It is the most important element in committing a crime, as mens rea means a "guilty mind" and without any guilty mind any person could not commit crime. Mens rea consists of many different mental thinking like recklessness and negligence.

How is Mens rea related to Internet crimes?
As Mens rea is needed for committing a crime, similarly in committing a cybercrime mens rea is needed. A hacker should have a wrong intention in hacking anybody else computer system or anybody's phone to which he is not authorised. Cybercrime does not only mean hacking, but it can be anything which is done against anybody without his/her will or consent on internet. It can be hacking or making any obscene thing against anyone, sending any offensive material etc.

There are two important essential ingredients to prove that it that there was mens rea:

1. There must be an unauthorised access to anyone's system
2. They must know about their act

The Cybercrimes through which Women are Mainly Affected:

Cyberstalking

It is very common nowadays for cybercrime against a woman [4]. It becomes easy to stalk a woman in internet than physically, as here the stalker does not give his original name or any original identity of what he is. The stalker can use any anonymous name to chat with any girl or woman. It is very easy to chat with a girl on internet hiding the identity or without coming in front of the girl.

Defamation
Cyber defamation includes defamation of both the kind LIBEL and SLANDER. In this the victim is victimize without even knowing that she is trapped [5]. Here the victim even does not even come to know that who defamed her, and her reputation is harmed.

Morphing
Morphing is highly increasing it is done by editing the original picture to misuse it. Perpetrators by accessing the internet download images or pictures of women or girls and use them to blackmail the women or girls by uploading them in social media or pornographic sites etc. [6].

Cyber-pornography
Is another threat to women because this includes publishing pornographic materials in pornography websites by using computers and internet wherein women will not even be aware of such immoral publication of their own very image [7]. This is done very secretly where the victim does not know the she has been victimized.

Pornography Addiction—Dr. Victor Cline, an expert on Sexual Addiction, found that there are four-step process among many who consume pornography.

- Addiction: Pornography provides a powerful sexual satisfaction effect, followed by sexual release, most often through masturbation.
- Escalation: Over time addicts require more new material to meet their sexual "needs."
- Desensitization: What was first perceived as gross, in time becomes common and acceptable.
- Acting out sexually: There is an increasing tendency to act out behaviours viewed in pornography.

Identity Theft
In this the identity of a person is stolen to do any crime or used to defame any person [8]. In the Perpetrators can steal anybody's identity to do a crime.

Phishing
Phishing is the attempt to gain sensitive information such as username and password and intent to gain personal information [9].

Trolling
It is a process in which the criminal tries to make conflicts by uploading false statements or any false picture or anything which can provoke the person against whom the statement is uploaded. Trolls are professional abusers who, by creating and using fake ids on social media, create a cold war atmosphere in the cyber space and are not even easy to trace [10].

Trojan Attack
The program that act like something useful but do the things that are quite damping. The programs of this kind are called as Trojans. The name Trojan Horse is popular. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the trojans use the UDP protocol as well.

Some precautions which a woman or girl should take:

1. Do not share passwords with anyone
2. Do not reveal everything to anyone on internet
3. Do not meet any online friends alone whom you are not acquainted
4. Always use antivirus on your system
5. Do not allow any unwanted application to access your system
6. Do not leave the webcam connected
7. Always update your applications
8. Before installing any application, you should read the terms and conditions carefully and other information provided.

CYBER LAWS AND NEED

Cyber Crime is not defined in Information Technology Act 2000 nor in the National Cyber Security Policy 2013 nor in any other regulation in India and it cannot be done in any way as it is a very wide aspect then what can be defined. Crime or offence is dealt and listed under the Indian Penal Code, 1860 with

the punishments and quite a few other legislations too. If anyone wants to define cybercrime then it can be said that any crime which takes place where a computer is been used or internet is used. To put it in simple terms 'any offence or crime in which a computer is used is a cyber-crime'. Cybercrimes can involve any type of crime or of any nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a new age crime that are addressed by the Information Technology Act, 2000.

Cybercrime can be further divided into two categories:

1. Using a computer to make another computer as target. For example – hacking, sending virus etc.
2. Using computers to commit a real-world crime. For example – cyber terrorism, credit card fraud, pornography etc.

To control these, cyber laws was introduced in the year 2000 as Information Technology Act 2000(IT Act 2000). Cyber law is very important as it covers all the aspects of transaction and activities which are related to internet.

Cyber law covers [11]:

1. Cyber crimes
2. Electronic and digital signatures
3. Intellectual property
4. Data protection and privacy

In today's world where internet or computers are used frequently, everyone is affected by the cyber laws. For example:

1. Almost all the transactions of shares are in the DEMAT (used to hold shares and take securities in electronic format) form.
2. In this generation all the companies and firms use computer and internet for keeping their date and to access it easily.
3. Government does its almost all work with the help of internet and computer, such as income tax return, form filling of any scheme etc.
4. Consumers are increasingly using credit/debit cards for shopping.
5. Most people are using email, phones and SMS messages for communication.
6. Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.

To safeguard everyone from being trapped by any hacker or anyone becomes a victim of cybercrime this cyber law was introduced. But unfortunately, all the citizens do not know about the law. And when they become a victim of cybercrime, they don't know what to do, where to register, how to register etc.

As per the cybercrime data maintained by National Crime Records Bureau (NCRB), a total of 217, 288, 420 and 966 Cyber Crime cases were registered under the Information Technology Act, 2000 during 2007, 2008, 2009 and 2010 respectively. Also, a total of 328, 176, 276 and 356 cases were registered under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007, 2008, 2009 and 2010 respectively. A total of 154, 178, 288, 799 persons were arrested under Information Technology Act 2000 during 2007-2010. A total number of 429, 195, 263 and 294 persons were arrested under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007-2010.

As per 2011 NCRB figures, there were 1791 cases registered under the IT Act during the year 2011 as compared to 966 cases during the previous year (2010) thereby reporting an increase of 854% in 2011 over 2010.

Of this, 19.5% cases (349 out of 1791 cases) were reported from Andhra Pradesh followed by Maharashtra (306), Kerala (227), Karnataka (151) and Rajasthan (122). And 46.1% (826 cases) of the total 1791 cases registered under IT Act, 2000 were related to loss/damage to computer resource/utility reported under hacking with computer systems [12]. According to NCRB, the police have recorded less than 5000; only 4829 cases and made fewer arrests (3187) between 2007 2011,

under both the Information Technology (IT) Act as well as the Indian Penal Code (IPC).

Actions that the Indian Government should take and Enforce to stop Cybercrime against Women

In India there are many laws which are being made for the betterment of the country, but they are not enforced or due to negligence of the politicians all those are not being followed. The government should make laws and made it available to every citizen of India. In India there are cyber laws but those are not known to the citizens, as what are they what they deal with, how to register complain under these laws, what offences are covered under these laws.

To make it clear the government should:

- Make relevant laws
- Make laws understandable to every citizen
- Make the laws available to every citizen(make it known to every citizen)
- Make the citizens know about the procedure to register their complains
- The punishment should be so strict for doing cybercrime that no other criminal think of doing it again
- Use their hackers and trackers to look after all the servers and if any unwanted activity is seen they should be tracked and should be punished within few days

Related laws are as follows:

- Section 67[13] deals with the publishing or generating obscene materials. And in the ITA act 2008 all the offences are included [14].
- Section 66A[15]: 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 are all covered here. Punishment for these types of acts is imprisonment up to three years or fine [16].
- Section 66B[17]: Dishonestly receiving stolen computer data or communication device has a punishment up to three years or one lakh rupees as fine or both [18].
- Section 66C [19]: Electronic signature or other identity theft are there like using others' password or electronic signature etc for any illegal work [20].
- Section 66D [21]: Cheating by person on using computer resource or a communication device shall be punished with imprisonment of either description for a term which extends to three years and shall also be liable to fine which may extend to one lakh rupee [22].
- Section 66E [23]: 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.
- Section 66F [24]: 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 [25].

Jurisdiction

The most important thing in deciding a cybercrime case is the jurisdiction, as it is too difficult to decide that which court will judge these cases. So according to Section 1(2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further Section 75 of the I.T. Act, 2000 also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section, the Act will apply to an offence contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. A Police Officer not below the rank of Deputy Superintendent of Police should only investigate any offence under this Act. (Sec. 78 of I.T Act, 2000). Without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction is a difficult proposition [26].

CONCLUSION

In India almost everyone is connected to internet, which makes it easy for the cyber criminals to attack anyone. India is a country where women are worshiped, but they are not only safe neither physically nor in internet. Cyber stalking is very common but unless some more severe violations like rape threat or revenge porn take place cyber stalking is not taken as a serious complaint and the complainant is often asked to block the stalker in different social media platforms. Our laws need to be changed to make them cyber-sensitive as well as gender sensitive [27]. Now the society that is dependent more on technology, so the crime based on internet law-breaking are bound to increase. So, the law makers should make the laws on that context and should be made known to the citizens.

REFERENCES

1. Available at<https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/>last visited on 15/03/2019
2. Available at<https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf> last visited on 15/03/2019
3. Available at<central law publication, cybercrimes and law, Dr.Amita Verma>
4. Available at<https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/> last visited on 15/03/2019
5. Ibid
6. Id
7. id
8. Available at< http://www.cyberlawsindia.net/index1.html>last visited on 17/03/2019
9. id
10. id
11. Available at<https://blog.ipleaders.in/need-know-cyber-laws-india/>last visited on17/03/2019
12. Id
13. Punishment for publishing or transmitting obscene material in electronic form. -Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
14. Id 6
15. 66A Punishment for sending offensive messages through communication service, etc. -Any person who sends, by means of a computer resource or a communication device,-(a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine. Explanation. For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.
16. id
17. Punishment for dishonestly receiving stolen computer resource or communication device. -Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to

believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

18. id
19. Punishment for identity theft. -Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.
20. id
21. Punishment for cheating by personation by using computer resource. -Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
22. id
23. Punishment for violation of privacy. -Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Explanation. -For the purposes of this section-

(a)"transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b)"capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c)"private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d)"publishes" means reproduction in the printed or electronic form and making it available for public; 9e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that;-he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

24. Computer related offences. -If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Explanation. -For the purposes of this section,-(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860); (b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).
25. Id
26. Available at <https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/10/8%20chapter%206.pdf> last visited on 19/03/2019
27. Available at<https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf> last visited on19/03/2019

Cite this Article
Pritam Mirdha, Md. Umar Faiz. Cyber Crimes against Women: Legal Precautions the Government Should Enforce in India. *National Journal of Cyber Security Law.* 2020; 3(1): 24–30p.