

# **CYBERCRIME AGAINST WOMEN, CHILDREN AND SENIOR CITIZEN**

*Written by Aishwarya Rajput*

*LL.M (Corporate and Commercial Law), Sharda University, Greater Noida, India*

---

## **ABSTRACT**

In present day scenario, the cybercrime is on the verge of rising and everyone is being a victim of such cybercrime which are happening worldwide by just a click on the computer and with the internet. The advance technology of the internet has definitely threatened the legality of the laws. Any person having an access to the internet and knowing how to operate a computer can easily commit the offence of cybercrime. Everyone has been a victim of cybercrime in their life sometime or the other. The existing norms and clauses of the criminal law seems to be ill equipped and outdated to deal with such advance crime happening in the cyberworld. Women and children have always been a target of any crime and likewise, the cybercrime against women has also taken the lead. Women are now also being subjected to the cybercrime and there have been many instances where we can see the females and the children being the easy target, even in the cyberworld.

In this paper I shall plan to discuss how the cyberworld has affected the women, children and senior citizen of the country. I shall also briefly examine upon various existing laws that deals with specific aspects of the cybercrime and also crime against women and children. I will be referring to various case laws to interpret the objectivity of the cybercrime and also refer the major sections of The Information Technology Act (2000) and The Indian Penal Code (1860). In this paper, I shall further describe what exactly a cybercrime is and what the various types of cybercrimes are. I will be elaborating the reasons of such offences and how an individual is being a victim under cybercrime, especially women, children and senior citizen. At our conclusion, we will focus on methods and judicial remedies available to prevent such cybercrimes.

**Keywords-** Cybercrime, Women, Children, Victim, Offence, Crime against Women

## **INTRODUCTION**

Cybercrime in general may be defined as ‘Any unlawful act where computer is used to commit or facilitate the crime. It includes all the criminal activities carried out by means of computer, and the internet.

The term ‘Cybercrime’ has been defined under Section 65 of The Information Technology Act (2000).

It is as follows:

### Section 65 of The IT Act (2000)

*a person who intentionally conceals or destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or network when the computer source is to be required to be maintained by law is punishable with imprisonment upto 3 years or with fine that may extend upto 2 lakh rupees or with both.*

*‘Computer source code’ means the listing of the programs, computer commands, designs and layout and program analysis or computer resource in any form.*

Crime is basically a social phenomenon and is as old as the civilization. With the growing advancement and rapid technology, most people have been a victim of cybercrime and other penal crime but women and children have always been an easy target due to the societal difference and growing concept of the men v/s women. The concept of cybercrime is not much different from that of the concept of conventional crime. Both include the breach of rules of law and counterbalance by the state.

## **CYBERCRIME AGAINST WOMEN**

Nowadays, crime against women and children is rising very rapidly and likewise, cybercrime against women and children is on the verge of rising. Most of the people are facing cybercrime

but almost every second, a woman is being a victim of such crime, reason being the disparity and the societal difference that some people have created for the women and also due to lack of proper knowledge.

The constitution of India guarantees equal rights to life, education, health, food and work to women but the same modesty of a woman seems to be diminished and no specific provisions have been made to protect the privacy or modesty of a women or children when facing any such cybercrime.

There are no specific provisions in the Information Technology Act (2000) for the cybercrimes committed against women and children. Cybercrime has thus become a hard reality in India, difficult to detect and also quite difficult to prevent. Paperless contracts, digital signatures, online transactions and cyber crime have taken the legal world by surprise. Most of the time, the perpetrators get a chance to harass, abuse or blackmail the women and children more because they tend to lack proper knowledge of dealing with cybercrime. The cybercrime against women is mostly done by creating fake accounts on social networking site such as Facebook, Twitter or Instagram. Women are also being trolled and objectified on many basis over the social media. The accused tend to post bad comments over the pictures of women and try to harass them by some sort of blackmailing, threatening or bullying.

It is hard reality of our nation that women are treated as objects and most men tend to suppress themselves over women because they think that it's some sort of a ritual or a rule that women need to be submissive to any male in their life and the male is always supposed is the main reasons which leads to cybercrime against women and children.

## **MAJOR FORMS OF CYBERCRIME AGAINST WOMEN**

Due to the commission of cybercrime, many women go through a lot of rough time in their lives and undergo hypertension, depression, anxiety and other adverse health issues. Women and children are the easiest target for perpetrators to commit crime against, be it conventional crime or the cybercrime.

Following is some of the most common cybercrimes that are committed against women and children worldwide. They are enumerated as below.

1. Cyber Stalking: This is a form of cybercrime which involves two persons, firstly the stalker, also called the attacker and secondly the women (victim) who is harassed by the stalker. Women nowadays have been the target of cyberstalking. It is basically a way to stalk or peep into someone's social media profile continuously, in an inappropriate way which directs to online harassment and online abuse. The cyberstalking involves using the internet, cell phone and any other electronic device used to stalk another person. Section 354D of The Indian Penal Code (1860) defines the term Cyberstalking.
2. Harassment through email: Harassment through email has become a very common type of cybercrime which is being conducted against women and children on a large scale. It includes bullying, threatening, cheating and blackmailing via email.
3. Phishing: Phishing is a type of social engineering where an attacker sends a false message created to manipulate the person with the intention to fraud them.
4. Cybersquatting: It is the practice of registering names, especially well-known companies or brand names, as internet domains, in the hope of reselling them at a profit.
5. Defamation: Cyber defamation includes libel as well as defamation. The offence of defamation is punishable under Section 500 of The Indian Penal Code with an imprisonment of upto 2 years or fine or both. The law of defamation under Section 499 got extended to "Speech" and "Documents" in electronic form with the enactment of the IT Act, 2000. The publication of material which intends to harm the reputation of the individual or organization, and such publication done via a computer and with the help of an internet, tends to constitute the offence of cyber defamation under the cyberworld.

6. Morphing: Morphing is simple editing the image of a person with a fake identity by an unauthorized person (the attacker) which is intended for some wrong purpose. The pictures of the females are downloaded by fake users and re-posted on the social media by creating fake profiles. The cybercriminals misuse the pictures of women by editing them with the morphing tools available on the internet and somehow promotes pornographic content.
7. Trolling: This is one of the most common cybercrime that is being committed against women and children in the cyberworld. Trolls spread conflicts and quarrels on the internet and the attacker posts bad or defamatory comments in an online community against the women which upsets them and causes severe anxiety, depression and other major health problems.
8. Child Pornography: Cyber pornography is another threat to the female netizens. There are various provisions under The Information Technology Act (2000) and The Indian Penal Code (1860) which regulates and prohibits child pornography. Section 67-B of the IT Act, 2000 makes publishing, transmitting, viewing or downloading child pornography illegal. Any person who has not attained the age of 18 years is a child. Section 292 of The Indian Penal Code prohibits the sale of obscene material. Also, the Protection of Children from Sexual Offences Act (2012) was enacted to protect children from the sexual offences. The act protects the children from sexual harassment, sexual assault and pornography. The act aims to protect the well being and interests of the children. The child pornography includes sexual content which intends to harm the modesty of a woman.

## **CASE LAW**

### ***The Ritu Kohli Case***

The Ritu Kohli case is the first case in India which was dealing with cyberstalking. The Delhi police arrested the culprit, Manish Kathuria. In the said case, Manish was stalking a person called Ritu Kohli by illegally chatting on a certain website. Manish was chatting under the



identity of Ritu Kohli and using obscene and obnoxious language. He was disturbing her residence telephone number and inviting to chat with her on telephone. Consequently, Ritu was getting obscene calls from other people, various parts of India and Abroad. Ritu Kohli reported the matter to the police and the Delhi Police swung into the action. The police had registered the case under Section 509 of The Indian Penal Code for outraging the modesty of a woman (Ritu). But Section 509 of the I.P.C only refers to words, gestures or act intended to insult the modesty of a woman. But when the same things are done on the internet, there are no such provision or mention about the same in the said section. Ritu Kohli's case was an alarm to the government to make laws regarding the aforesaid crime and regarding protection of victims under the same.

As a result, Section 66A of the Information Technology Act, 2008 states, "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 makes by making use of such computer resource or a communication device,
- (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.

## **CYBERCRIME AGAINST SENIOR CITIZEN**

Like women and children, even senior citizens are also being targeted as a victim of cybercrime. Usually, the reason being that they lack the exact knowledge about the technology. They are not much aware about how to go along with the advanced technology of the internet

and computers and hence, they too become the easy targets of cybercrime. Here are some forms of cybercrime that are committed against the senior citizens:

1. Government impersonation scam: The attackers or the criminals impersonate themselves as government employees and asks for money by threatening or blackmailing the old citizens. Unaware about such crimes, the senior citizens tend to fall into their trap of cybercrime.
2. Financial scam: Criminals target potential victims using illegitimate credentials from legitimate services.
3. Cyberextortion: Under this crime, the attacker or the criminal asks or extorts for money from the senior citizens by blackmailing them on the basis of certain grounds.

## **PREVENTION OF CYBERCRIME**

The cybercrime against women, children and senior citizen is on the verge of rising and they are being attacked by the attackers across the globe. The Ministry of Home Affairs has initiated a scheme for the prevention of cybercrime against women and children and a mechanism to deal with the same.

Following are the components of the CCPWC scheme:

- Online cybercrime reporting unit
- Forensic unit
- Capacity building unit
- Research and development unit
- Awareness creation unit

## **PREVENTIVE MEASURES PROVIDED BY THE GOVERNMENT**

1. LEGISLATIVE SUGGESTIONS: Special provisions need to be passed by the legislature which shall specifically deal with the cybercrime against women and children.

2. JUDICIAL SUGGESTIONS: A special bench of judges should be appointed in each High Court which shall specifically deal with the cases related to cybercrime against women, children and senior citizens.

## **SUGGESTIONS TO PREVENT CYBERCRIME**

1. Always use strong passwords and do not share the passwords or username with any person
2. Proper knowledge regarding the use of the internet and computer should be imparted to everyone, especially the women and the children
3. Specific laws should be made by the legislature and shall be implemented in the nation
4. Avoid meeting any online friend alone as they are a complete stranger. Always prefer taking some trustworthy person along if ever meeting an online friend face to face
5. Block the person if he/she talks in an inappropriate way which targets the modesty or any other aspect which can be harmed
6. Limit the amount of personal information that you post on your social media
7. Avoid adding unknown people to your social networking sites such as Facebook, Instagram, Twitter or Whatsapp
8. Never send money or any personal bank details to any unverified person on the internet
9. Never share financial account or bank account details and do not allow anyone to access your accounts
10. Never open any attachment links from an unknown or unauthorized email address

## **CONCLUSION**

To sum up, we can say that cybercrime is a very ongoing type of a crime which is happening worldwide. The digital platform and social media are the main tools that are used to commit cybercrime. One needs to be very cautious and careful when using social media and accessing the internet. Women, children and the senior citizens need to be even more careful while using the social media because they are the ones who are largely targeted by the attackers. One should



avoid sharing personal details on the social networking sites. Women need to be more courageous in reporting any type of unusual activity that they notice online. Although we have certain provision of the Information Technology Act and The Indian Penal Code which somewhat deals with the offence of cybercrime but there needs to be proper and specific provisions which clearly mentions and describes the cybercrime against women, children and the senior citizens.

## REFERENCES

- The Information Technology Act, (2000) Section 65
- The Information Technology Act, (2000) Section 66
- The Information Technology Act (2000) Section 66-A
- The Information Technology Act (2000) Section 67-B
- The Indian Penal Code (1860) Section 292
- The Indian Penal Code (1860) Section 354-D
- The Indian Penal Code (1860) Section 500
- The Indian Penal Code (1860) Section 509
- The Protection of Children from Sexual Offences Act, 2012
- The Ritu Kohli Case