

## **CYBER LAWS IN INDIA: YOUR RIGHTS AND REMEDIES**

Rooby Karumannil

III Semester MSc Computer Science Student, PG Department of Computer Science

Ansar Women's College, Perumpilavu Contact: 9846374055

email id: [roobykarumannil@gmail.com](mailto:roobykarumannil@gmail.com)

### **ABSTRACT**

*This article is on the topic "Cyber Laws In India: Your Rights And Remedies" by Rooby Karumannil. In the emerging tech world, people are becoming more and more digitally developed and so are the crimes. Internet was actually developed as information tool and mainly used for research. But now a day, it is more used for other purpose like e-business, e-commerce, e-governance and e-procurement etc. All legal issues and crimes related to internet are dealt through cyber laws. The number of internet users is at the upward thrust, the need for cyber laws and their application has broadly increasing. Sometimes the victims can't get over from the trauma, they were haunted by lifelong. In this updated world and increasing complexity of the technological world we should know all the cyber laws in India. So that we can know our rights and we will be more concerned about the remedies. By this article my aim is to showcase the cyber laws under INDIAN PENAL CODE(IPC) how to protect oneself from all these networks.*

**KEYWORDS:** Cybercrimes, Cyber laws

### **INTRODUCTION**

Now is a good time as any to understand sexual assault in the realm of digital life. We often use the terms online harassment and online abuse interchangeably. Cybercrimes are basically crimes that happen under the blanket of internet, in which the offender is blanketed by the veil of pc display and may not disclose their identity. There is no formal definition for cyber sexual harassment, but we can say that any behaviour that aims at damaging a person's

reputation, feelings, self-esteem and mental health is sexual assault. The harassers would possibly incite fear of physical harm, supply threats submit something defamatory about the victim. Cyber criminals use computer technology to access personal information and use internet for harassment and explanation purpose which including stalking, blackmailing, threatening via emails, photo morphing, cyber pornography etc.

Cyber sexual harassment can be of many types. It includes cyber stalking, which means a person (known or unknown) send abusive, threatening or unwanted messages to a victim by any communication system. Next, we can say that gender harassment, it involves any unkind and disrespectful remark made to a person based on their gender. Cyber bullying can include such acts as making threats, insulting them, slut shaming attempt to hack other computers etc. There are so many other harassments too, such as identity theft, privacy violation, voyeurism and revenge pornography.

As of February 2022, India is the country with the second-largest internet population in the world. India's cybercrime cost Rs.1.25 lakh crore in 2019, putting India second among nations that suffered from cyber attacks between 2016 and 2018. Online cracking or denial-of-service attacks are examples of gaining access to a computer system without permission or without using the location of criminal activity to carry out the activity. There are numerous vulnerabilities in gadgets along with mobile phones that people use to get admission to services. An exam of the assault vector in a cell smartphone determined that aside from the packages, there are 15 distinct factors via which a hacker might fit access to it. Bluetooth, verbal exchange modules, microchips, running systems, CPUs are all examples. By exploiting the inadequate IT infrastructure at employees' homes, hackers have devised a number of ways to acquire passwords. Despite an increase in cyber attacks, 7 lakh intrusions have been documented through August of this year, an increase of 175 percent over the same period in 2014.

## CYBER SEXUAL VIOLENCE IN INDIA

India has one of the fastest growing social media platform presences in the world with different type of users engaging with various activities in social media itself. There was a newspaper publication in 2017 claimed that four out of five people in India had experienced online harassment in different form. Notwithstanding the platform, social media users may find themselves caught in the situation of online bullying. Main issue among these days are people hiding their identity and forwarding indecent comments under our social media posts. Also, many women whom I know have received frequent and sometimes aggressive messages from total strangers over the internet on different platform. These indecent behaviours are very common now and people are unaware about the consequence. So, the main theme about this article is to bring awareness about the cyber sexual violence and the remedies for those attacks also the precaution. By exploiting flaws in IT security mechanisms, they hack sensitive information. There are several reasons why IT platforms are so vulnerable:

**Accessibility** - Because of the complexity of tech, there exist many ways to breach a pc method. Computer criminals can access permission codes, advanced articulate recorders, retina scans, and other information that might be utilized to avoid security measures.

**Complicated codes** - Functioning systems are utilized to run computers, and these functioning systems are composed up of millions of lines of code. Because the human intellect is flawed, mistakes can happen at any time and in such cases, cybercriminals take benefit of any code mistake.

**Aptitude to store information in a comparatively little space** - A pc has the original aptitude to store information in an extremely small space. This makes it easier for someone to take information from other storage devices and utilise it for private acquire.

**Carelessness** - Part of the hallmarks of human behaviour is negligence. As a consequence of, there exists serendipity that when securing the pc treat, we may make a error that lets cyber-criminal permission and temperance over the pc scheme.

**Evidence loss** - Information narrating to the crime might be readily deleted. As a consequence of, evidence loss has become a extremely widespread and apparent issue that paralyses the mechanism behind the cyber-crime investigation.

#### WHAT ARE THE CYBER HARASSMENT LAWS IN INDIA

There are so many cyber harassment laws in India, among those few of them are under the cyber sexual harassment laws in India under 'THE INDIAN PENAL CODE, 1980' (IPC). Section 298 criminalizes about the hate speeches aimed at damaging the religious sentiments of individuals. The victim can file case against them if they found any damages against their images. Next section under IPC is 354A proscribes that many forms of sexual harassment like forcefully showing any unwanted things like pornography or nudity or making unwelcome physical contact and sexual advances. I think this section is very important in the cyber harassment, because most teenagers are facing these issues among these social media worlds. Section 354C makes voyeurism a punishable offence. It includes taking videos or watching of people who is under any private activity like sexual intimacy or bathing. This were also very common now a days. Section 354D punishes for every form of stalking including social media stalking. This is a serious issue to discuss. Because social media stalking is very common now. And people are unaware that they are doing a big crime. But in this case people will not caught if they state their innocent, and purpose of stalking with clear and detailed proof. Section 499 under IPC criminalizes defamation, or the act of tarnishing of an individual's reputation through words, action, signs or any kind of activity. Section 503, 506 and 507 proscribes criminal intimidation by forcefully doing unwanted

things. Section 509 under IPC criminalizes insulting the modesty of a woman through any act, gesture, or word and violating her privacy life to destroy their peaceful life knowingly.

In 2018, a cyber-attack on the Cosmos bank in Pune frightened the complete banking industry. Computer criminals stole Rs 94.42 crore by smashing into the bank's ATM server and stealing the private details of abundant debit cardholders. Money was stolen, and computer criminals from 28 nations without further ado dropped it. In 2018 again a massive information breach entailing 1.one billion Aadhar card users occurred. The hacked information contained personalized details as an example Aadhar, cellphone, PAN, and bank account numbers, along with IFSC codes. Surprisingly, unknown merchants were rapidly selling Aadhar details on WhatsApp for Rs 500 per individual. Moreover, for a meagre Rs 300, one could inherit a printout of anyone's Aadhar card.

#### INFORMATION TECHNOLOGY ACT, 2000

We have separate IT ACT , 2000 under IPC other than cyber harassment laws. Section 66C makes identity theft using fraudulent for dishonest means a punishable offence. Section 66E criminalizes the intentional capture, publication or booklet, or dissemination of the images of the private areas of any person without his/her consent. This section protects victims of all genders. Section 66F deals with act of cyber terrorism including Dos attacks and the hacking of electronic devices. Section 67 makes any publication or transmission materials over electronic medium a punishable offence. Section 67A forbids transmission or publication of sexually explicit act or any unkind activity conduct over electronic media.

Other than IT ACT we have separate laws or act for INDECENT REPRESENTATION OF WOMEN (prohibition) ACT, 1986. Section 4 bars the production, distribution or circulation of any materials containing indecent representation of women in any form. Next special laws for women are THE SEXUAL HARASSMENT OF WOMEN AT WORKPLACE ACT, 2013.

We know that 7 out of women are facing sexual harassment at their workplace. So, every woman especially men should be aware about these rules that aimed for preventing sexual harassment of women. Section 2(n) defines “sexual harassment” but does no longer specify any medium. Besides, section 2(O) defines “workplace or place of job” to include “a residence” as well.

## REMEDIES

The main remedies for these issue for now a day, the centre for advanced research in Digital Forensics and Cyber Security (ARDC) recommends three options to explore. They are social media websites, the National Commision for Women, and Cyber cells. We should be aware that these are one among the remedies for our issues. Also, we should be more aware about our social media websites and should conduct awareness on different platform. So that we would be more conscious. Also, we can contact at [complaintcell-new@nic.in](mailto:complaintcell-new@nic.in) or call at 011-26944883 and 011-26944880. These all are available for everyone at any time. Also, we can contact the ministry by calling at +91-11-23381611 or by sending an email at [nic-mwcd@gov.in](mailto:nic-mwcd@gov.in). Other than that under-secretary at the ministry at [bbb.shankar60@gov.in](mailto:bbb.shankar60@gov.in) or +91-11-23381611.

## THINK TWICE

We should be more conscious about our security. We can't compromise on our security. It acts the wall for our home. It secures our all the gadget and systems. Also always keep the information private. And be cautious about what we share and what others see through our social media account. Do not click unwanted links or messages. Also please try to read all the instruction before you install any new apps or software and try to give permission to only the needed things. Make sure you really need those. Also always cover

your camera on everything. That makes your private life more secure. In most cases our system will get hacked and they were watching for hours. After that they ask for money. Before all these happening, be present minded and keep a genuine antivirus installed. By all these steps we will be more secured than previous. Replace the Wi-Fi network's default pass code to something more procure. Restrain the number of devices that may associate to the Wi-Fi network and only let lawful devices to get connected. Be sure to modify all the systems and programs, along with to install and gain an antivirus application up to up now. Information backup must be a daily tasks arrangement since information may be rapidly destroyed, contaminated, or manipulated.

## **CONCLUSION**

By the past few years there is a huge growth in cybercrimes. India recorded 16% jump in the number of cyber-attacks in India. Most cyber-attacks are very common now and people are also doing some of them and unaware about it. So, this article indents to bring an awareness about the cyber-attacks and their laws under Indian Penal Cord. As people's reliance on tech grows, cyber laws in bharat and around the world need to be always updated and subtle. The pandemic has additionally guided a big part of the workforce into a distant working mode, intensifying the need for app security. Legislators need to go overhead and above to maintain ahead of the impostors and cease them in their tracks. Cyber crime might be coped, but it takes the combined efforts of authorities, web or network providers, intermediaries as an example banks and shopping sites, and more importantly crucially, consumers.

## REFERENCES

- [1] Harshit Agarwal, (2020, July 15), " Everything About Cyber Laws in India", appknox.  
<https://www.appknox.com/blog/cybersecurity-laws-in-india>
- [2] Vinay Deep, (2020, April 3), " Online Harassment Laws In India : Your Rights And Remedies", Legopedia. <https://legodesk.com/legopedia/online-harassment-laws-in-india-your-rights-remedies/>
- [3] Harika Tejavath, (2020, April 28), " Cyber Sexual Harassment Laws in India ", Legal Bites. <https://www.legalbites.in/cyber-sexual-harassment-laws-india/?infinitemscroll=1>
- [4] Nica Latto, (2022, February 2), "What Is Cyber Crimes And How Can You Prevent It", Avast. <https://www.avast.com/c-cybercrime>
- [5] Swati Shalini (2019, September 12), "How To Prevent Cyber Crimes In India" Myadvo. <https://www.myadvo.in/blog/cyber-crime-in-india/>