International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 2, January-February 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Crimes and Cyber Laws in India: An Overview

Dr. S. Krishnan[1], Mr Harsh Shrivastava[2]

[1]Associate Professor, Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India
[2]Assistant Professor, School of Engineering, Jaipur National University, Jaipur, Rajasthan, India

ABSTRACT

Internet, the worldwide connection of loosely held networks, has made the flow of data and information between different networks easier. With data and information being transferred between networks at distant locations, security issues have become a major concern from the past few years. The internet has also been used by few people for criminal activities like unauthorized access to others networks, scams, etc. These criminal activities related to the internet are termed as Cyber Crimes. With the increasing popularity of online activities like online banking, online shopping, etc., it is a term that we often hear in the news now-a-days. Therefore, in order to stop and punish the cyber criminals, "Cyber Law" was introduced. Cyber Law can be defined as law of the web, i.e., it is a part of the legal systems that deals with the Internet, Cyberspace and with other legal issues like online security or online privacy.

Therefore, keeping the objectives in mind, this chapter is divided into different sections in order to provide a brief overview of what is cybercrime, the perpetrators of cybercrime-hackers and crackers, different types of cybercrimes and the evolution of cyber laws in India. The chapter further throws light on how these laws work and the various preventive measures which can be used to combat this "hi-tech" crime in India.

How to cite this paper: Dr. S. Krishnan | Mr Harsh Shrivastava "Cyber Crimes and Cyber Laws in India: An Overview" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-2, February 2022, pp.792-798, URL: www.ijtsrd.com/papers/ijtsrd49324.pdf

IJTSRD49324

KEYWORDS: *Internet, Cyber Crime, Cyber Law, Cyberspace, Online security, Online privacy, Hi-Tech Crime, Hackers, Crackers, Unauthorized access*

INTRODUCTION

A computer can be defined as the machine that stores and processes information that are instructed by the user. Cyberspace, i.e., the Internet, has made the flow of data and information between different networks easier and more effective. The internet technology is used for various purposes ranging from online dealing to online transactions. Since decades majority computer users are utilizing the computer, either for their personal benefits or for other benefits. Therefore, security related issues have become a major concern for the administrators. This has given birth to "Cyber Crimes". Cyber Crime can thus, be defined as the crimes committed by using computer or computer network and usually take place over the cyberspace especially, the Internet. In simple terms, cybercrimes are the offences that take place over electronic communications or information systems. A Cybercriminal may use a device to have access to users' personal information, confidential business information, and government information or to disable a device. Selling any private data or information without the consent of the owner also falls under cybercrime. Criminals performing such activities are often referred to as hackers. *Therefore, cybercrimes are also known as electronic crimes or e-crimes, computer-related crimes, high-tech crime, digital crime and the new age crime.*

Today, Cybercrime has caused a lot of damages to individuals, organizations and even the Government. Several laws and methods have been introduced in order to stop crimes related to the Internet. *"Cyber Law"* was introduced in India with an objective to cover the part of the legal systems that deals with the Cyberspace and legal issues, online security or online privacy, etc. In other words, Cyber Law can be defined as the laws that govern the Cyberspace cybercrimes, digital and electronic signatures, data

protections and privacy, etc., and comprehended by the cyber law. The UN's General Assembly recommended the first Information Technology (IT) Act of India in 2000. This Act was passed on the "United Nations Model Law on Electronic Commerce (UNCITRAL) Model".

OBJECTIVES:

This qualitative Research Paper has been written keeping in mind the following three main objectives:

1. To spread knowledge on the crimes/criminal activities like unauthorized access to others networks, scams, etc., that are taking place through cyberspace especially, the Internet;
2. Generate awareness among the masses on "Cyber laws" that are imposed in order to stop the cybercrime and/or punish the cyber criminals; and
3. To suggest other preventive measures apart from the Cyber Law so that there can be safety of the users in the cyberspace.

WHAT IS CYBER CRIME?

Sussman and Heuston was the first to propose the term "Cyber Crime" in the year 1995. Cybercrime has no single definition; it is considered as a collection of acts or conduct- these acts are based on the material offence object and modus operandi that affect computer data or systems[1]. By definition, Cybercrimes are *"criminal acts implemented through use of a computer or other form of electronic communications"* (Anderson & Gardener, 2015).In simple words, acts which are punishable by the Information Technology (IT) Act, 2000 are known as "Cyber Crimes". In India, the IT Act, 2000 deals with the cybercrime problems. Certain amendments were made in this Act in 2008; thereby passing the Information Technology (IT) Act, 2008 covering a wide range of area such as online commercial transactions, digital signatures, e-commerce, etc.

Therefore, "Cyber Crime" can be defined as any malefactor or other offences where electronic communications or information systems, including any device or the Internet or both or more of them are involved[2].

THE PERPETRATORS-HACKERS AND CRACKERS:

1. **Hacker:** According to *Section 66A of Information Technology (IT) Act, 2000*[3], a person whosoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or effects it injuriously by any means is a hacker.
2. **Crackers:** According to the *Jargon Dictionary*[4], the term "cracker" is used to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. In other words, a "cracker" is defined as a hacker with criminal intent who maliciously sabotages computers, steal information located on secure computers and cause disruption to the networks for personal or political motives.

CLASSIFICATION OF CYBER CRIMES:

Information technology has been misused for criminal activities in today's world. Such crimes may be committed against the governments, individuals and institutions. Various types of cybercrimes exist in India and all over the World. The common types of cybercrimes are discussed as follows:

1. **Hacking:** It simply refers to have an unauthorized access to another computer system. It is the most dangerous and commonly known cybercrime. The hackers break down into the computers system and steal valuable information, known as data, from the system without any permission. Hacking can be done for multiple purposes like data theft, fraud, destruction of data, and causing damage to computer system for personal gains. Therefore, hackers are able to spoof the data and duplicate the IP address illegally.

According to the research committed by the SANS Institute (2004), there are 3 different types of hackers:

- **White Hat Hackers:** These are the ethical hackers that use their hacking skills for good reasons and do not harm the computer system.
- **Black Hat Hackers:** These types of hackers use their computer knowledge to gain unauthorized access to a computer system with a malicious or harmful intention. They may steal, modify or erase data, and insert viruses and damage the system.
- **Grey Hat Hackers:** They are the skilled hackers that usually do not hack for personal gains. Therefore, they are hybrids between white hat and black hat hackers[5].

2. **Cyber Terrorism:** It refers to unlawful attacks against computers, networks and the information stored therein that are carried out to intermediates

[1] United Nations Office on Drugs and Crime – UNODC (2013)
[2] http://cybercrime.org.za/definition
[3] http://cyberlawsinindia.net/black-html.7/4/2015
[4] The Jargon Dictionary on website http://www.netmeg.net/jargon/terms/c/cracker.html
[5] https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-grey-1390

or coerce a country's government or citizens, having political or social objectives. Therefore, terrorism acts which are committed in cyberspace are called cyber terrorism[6]. The cyber terrorism attacks and threats include:

- **Cyber Warfare:** It is an Internet based conflict which involves politically motivated attacks on the computer system. Such attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems, among many other possibilities.
- **Malicious Software:** These are Internet-based software or programs that can be used to gain access to a system to steal sensitive information or data or disrupt the software present in computer system.
- **Domain Hijacking:** It refers to the act of changing the registration of a domain name without the permission of its original registrant.

3. **Cyber Stalking:** It is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. It is a willful conduct by the cyber stalkers through any online medium like email, social media, chatrooms, etc., that actually causes the victim to feel frightened, intimidated or molested. Usually the stalker knows their victim and majority of the victims are women.

Earlier, the cyber stalkers were booked under Section 509 of the IPC due to lack of punishment under the IT Act, 2000. After the Amendment of the IT Act in 2008, the cases involving cyber stalking can be charged under Section 66A of the Act and the offender is punishable with imprisonment up to three years, and with fine.

4. **Cyber Bullying:** According to the Oxford Dictionary[7], Cyber Bullying can be defined as the *"use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature"*. It occurs when children including teenagers are threatened, harassed, humiliated, or otherwise targeted by other children using digital technologies. Cyber bullying may arise to the level of a cyber harassment charge, or if the child is young enough it may result in the charge of juvenile delinquency[8].

Due to the increasing utilization of cell phones now-a-days, parents should keep a check on the mood swings of their children. Rather, they should get more involved in their online activities in order to safeguard them from cyber bullying.

5. **Cyber Pornography:** It refers to the act of using cyberspace to create, display, distribute, or publish pornography or obscene materials. In other words, stimulating sexual or other erotic activities over the Cyberspace, especially the internet is known as Cyber Pornography[9]. Many websites exhibit pornographic photos, videos, etc., which can be produced quickly and cheaply either through morphing or through sexual exploitation of women and children. *Morphing* refers to the editing of an original picture through a fake identity or by an unauthorized user which is punishable under IPC and Section 66 of the IT Act, 2000.

Child pornography is abundant on the internet. Online child pornography involves underage persons being lured into pornographic productions or being sold or forced into cybersex or lives of prostitution (CNN staff author, 2001). Kidnapping and international smuggling of young girls and boys for these purposes is now a transnational crime phenomenon often instigated in impoverished nations where victims face dire economic circumstances (Chinov, 2000).

6. **Cyber Theft:** It is another form of cybercrime used by the cyber criminals to steal information or money from a distant location with the help of a computer or an internet. It includes various types of crimes like:

- **Identity Theft:** It refers to the fraud which an individual does by making a fake identity on the internet in order to steal money from bank accounts, credit or debit cards, etc. It is punishable offence under Section 66C of the IT Act, 2008[10].
- **Phishing:** It is a another very common type of cybercrime which is used by hackers to steal information which is personal like passwords, usernames, bank account number, credit card details, etc. It is generally carried out with the help of email spoofing.

[6] https://www.britannica.com/EBchecked/topic/130595/Cybercrime

[7] https://www.lexico.com/definition/cyberbullying

[8] https://stopcyberbullying.org/what-is-cyberbullying-exactly.html.21/3/2015

[9] http://www.yourdictonary.com/cyberpornography

[10] https://cybercrimelawyer.wordpress.com?category/66-c-punishment-for-identity-theft/

- **Forgery:** It means making of false document, signature, currency, revenue stamp, etc.
- **Web jacking:** It refers to hi jacking of the victims account with the help of a fake website in order to damage it or change the information of the victims' webpage. The attacker sends a link to the victims email. When the victim opens the link, a new page appears with the message of clicking another link. By clicking on the link, the victim will be redirected to a fake page.
- **Cyber Embezzlement:** Such type of crime is performed by employers who already have legitimate access to the company's computerized system. An employee may perform such a crime in order to earn more money.
- **Corporate Espionage:** This is a type of crime committed by individuals in order to gain competitive advantage in the market. Under this crime, the cybercriminal may be from within or outside the company and he/she may use the company's network to steal the list of clients, marketing strategies, financial data, trade secrets, etc.
- **Plagiarism:** It is used to steal someone else original writings and call it as their own. Since most of the data is available online and people are now having more access to the internet and the computers, the problem of plagiarism is increasing day-by-day. There are certain software's that are used to detect plagiarism.

7. **Email Spoofing:** According to Techopedia, email spoofing is a fraudulent email activity/technique used to hide the original address of the email message, although the mail appears to have come from a legitimate source[11]. It is very common now-a-days. Such tactics are usually done by spammers having malicious intentions such as to gain access to someone's banking information or to spread virus. The offender is charged with *forgery* under Section 463 of the IPC for committing such offences.

SMS Spoofing is also found in today's modern world of technology. It allows changing the name or number text messages appear to have come from.

PREVENTION OF CYBER CRIMES:

In order to stop crimes committed through the computer resources and Internet technology, "Cyber Law" was introduced. "Cyber Laws" can be defined as the legal issues that are related to the utilization of communication technology, concretely "cyberspace", i.e. the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, each action in Cyberspace has some legal and cyber legal views[12].

Based on the United Nations Model Law on Electronic Commerce (UNCITRAL), 1996, the Indian Parliament passed the *Information Technology Act, 2000* (also known as the IT Act no. 21 of 2000) on 17th October, 2000. This law was introduced in India to deal with the digital crimes or cybercrimes and electronic commerce.

Some key points of the Information Technology (IT) Act, 2000 are as follows:

- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- The Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through e-governance.
- The communication between the companies or between the company and the government can now be through internet also.
- Addressing the issue of security is the most important feature of this Act. It introduced the concept of digital signatures that verifies the identity of an individual on the internet.
- In case of any loss or harm done to the company by criminals, the Act provides a remedy in the form of money to the company.

Since the Information Technology Act, 2000 did not covered all the aspects of cybercrimes committed; amendments were done in the Rajya Sabha on 23rd December, 2008, renaming the Act as the Information Technology (Amendment) Act, 2008 and was referred to as ITAA, 2008. Eight new Cyber Offences were added to ITAA, 2008 under the following sections:

[11] https://www.techopedia.com/definition/1664/email-spoofing

[12] https://www.cyberlawsindia.net//cyber-india-html

Sr. No.	Sections under the Information Technology (Amendment) Act, 2008	Punishment
1.	**Section 66A:***Cyber Stalking*, i.e., sending offensive messages through any communication services like a computer or mobile phone	Imprisonment up to 3 years long with a fine.
2.	**Section 66B:***Receiving stolen computer's resources or communication device dishonestly*	Imprisonment which may extend up to 3 years, or with a fine of rupee 1 lakh or both.
3.	**Section 66C:***Identity Theft*	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
4.	**Section 66D:***Phishing,* i.e., punishment for cheating by personation by the use of computer's resources	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
5.	**Section 66E:***Voyeurism,* i.e. punishment for violating privacy of an individual	Imprisonment for 3 years along with a fine which may be extended up to 2 lakh rupees or both.
6.	**Section 66F:***Cyber Terrorism*	Life imprisonment.
7.	**Section 67A:***Publishing/ or transmitting material in electronic form containing sexually explicit contents*	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first convict; and imprisonment can be extended up to 7 years with fine of 20 lakh rupees in the second convict.
8.	**Section 67B:***Child pornography*	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first conviction; and imprisonment can be extended up to 7 years with an extended fine of 10 lakh rupees in the second conviction.

Following are some of the *important Sections under Indian Penal Code* for protection of individuals from Cybercrimes:

Sr. No.	Sections under Indian Penal Code (IPC)	Punishment
1.	**Section 354A** punishes the offence of *Sexual Harassment*	3 years of imprisonment and/or fine.
2.	**Section 354C**criminalizes the offence of *Voyeurism,* i.e., the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her consent	3 years of imprisonment for the first conviction and 7 years of imprisonment on the second conviction along with fine.
3.	**Section 503** punishes *Criminal Intimidation* as threats made to any person with injury to her reputation	Imprisonment which may extend up to 2 years, and/or fine.
4.	**Section 507**punishes *Criminal Intimidation* by an anonymous communication	Imprisonment which may extent up to two years.
5.	**Section 228A**deals with *vengeful posting of images or videos of rape victims*	Imprisonment which may extend up to two years and fine.

Apart from the above mentioned Sections under the IPC and ITAA, 2008, the Government of India has taken the following steps for prevention of Cybercrimes:

- *Cybercrime cells* have been set up in states and U.T's for reporting and investigation of Cybercrime cases.
- The Government under the IT Act, 2000 has also set up *Cyber Forensic and Training Labs* in states of Kerala, Assam, Mumbai, Mizoram, Manipur, Nagaland, Arunachal Pradesh, etc., for awareness creation and training against Cybercrimes.
- In collaboration with Data Security Council of India (DSCI), NASSCOM, *Cyber Forensic Labs* have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training.
- Various programs have been conducted by the Government of India to generate awareness about Cybercrimes. *National Law School, Bengaluru* and *NALSAR University of Law, Hyderabad*are

engaged in conducting several awareness and training programs on Cyber Laws and Cybercrimes for Judicial officers.

Training is imparted to Police officers and Judicial officers in the *Training Labs* established by the Government.[13]

OTHER PREVENTIVE MEASURES:

Due to borderless nature of Cybercrimes, innovative measures are required to curb the issue of "hi-tech crime". Therefore, apart from the Cyber Laws, one should keep the following points in mind for safety in Cyberspace while surfing the Internet:

1. Awareness should be generated among the students at the grassroot level, i.e., knowledge about cybercrimes and cyber laws. Cyber literacy should be given to the students in Computer Centers, Schools, Colleges and Universities as well. Cyber Law awareness programme can be organized in any educational institute in order to provide basic knowledge of Internet and Internet's security.
2. Bank and Credit Card statements should be reviewed on regular basis to reduce the impact of identity theft and crimes committed online.
3. Keep your computer system up-to-date in order to keep attackers away from your computer. By keeping your computer updated, you block attackers from being able to take advantage of software flaws that they could otherwise use to enter into your system and hack it for illegal purposes.
4. Unique and strong passwords of eight characters by using a combination of symbols, words and figures, should be kept for online activities like online banking. Avoid using your email id, login name, last name, date of birth, month of birth or any such personal information as your passwords that can be traced easily.
5. Same passwords should not be kept for every online service you use. Keep different passwords for different online activities.
6. Enable Two-step Authentication in the webmail in order to make your webmail or social media account secured. Add mobile no. to your mail account so that you get notified in case someone else tries to gain access to your account.

Under Two-step Authentication, your username and password is required to open your account. But, a verification code is sent to your registered mobile no. in case you forget your password for personal security purposes. A hacker may be able to crack your password but without the temporary verification code, he/she cannot have access to your account.

7. For basic online security, your computer must be protected by security software since the software helps to protect from online threats. Therefore, these softwares are essential for staying safe on the Internet. It includes Firewall and Antivirus programs. Firewall controls who and what can communicate with your computer online. Antivirus also maintains all online activities such as email messages and web browsing and protects the system from viruses, worms, Trojans horse and other types of malicious programs.

Integrated security programs such as Norton Internet Security combine Firewall, Antivirus, Antispyware with other features such as Antispam and parental controls have become popular now-a-days since they offer all the security software needed for online protection in a single package.

viii. Do not respond to emails that ask for personal information and don't click on the links in these messages as they may take you to fraudulent and malicious websites. Pay attention to privacy policy on Websites and in software before you share your data with them because legitimate companies do not use email messages to ask for your personal information.

CONCLUSION:

To conclude, we can say that the advent computer networking and newly developed technologies have given rise to cybercrimes in the past few years. This has created great threats to mankind because the victim is known to the attacker and he/she with malicious intentions like causing harm to the computer system, stealing or erasing data saved in the system, changing password, hacking credit card details, and bank account number, etc., commits such crimes. Different types of cybercrimes like cyber stalking, cyber terrorism, cyber pornography, morphing, forgery, email spoofing, identity theft, etc., have serious impacts over the society. The cybercriminal gains unauthorized access to computer resources or any other personal information of the victim by hacking their account. It is, therefore, very important for every individual to be aware of these crimes and remain alert and active to avoid any personal or professional loss.

[13] https://books.google.co.in/books?id=TDLWCwAAQBAJ&pg=PA59&lpg=PA59&dq=cyber+forensics+and+training+labs+in+states+of+kerala+assam+under+the+information+technology+act+2000&source=bl&ots=fhUt95iXD8&sig=ACfU3U2Yx8GSZBwoGLAtnRXihiZbRpi55A&hl=en&sa=X&ved=2ahUKEwiR4Zqnwc7nAhWDf30KHS78AgMQ6AEwAHoECAYQAQ#v=onepage&q=cyber%20forensics%20and%20training%20labs%20in%20states%20of%20kerala%20assam%20under%20the%20information%20technology%20act%202000&f=false

However, in order to solve the problem of Cybercrime having global dimensions, the government of India enacted the Information Technology Act in 2000 to deal with such "hi-tech" crimes. The Act was passed again in 2008 with certain amendments. Eight new offences were added and the Act was renamed as the Information Technology (Amendment) Act, 2008 referred to as ITAA, 2008. Apart from this act, certain Sections under the Indian Penal Code (IPC) are also used as legal measures to punish the individuals committing such crimes. Legal provisions on Cyber Stalking and Online Harassment are also included under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. Thus, to ensure justice to the victims and punish the criminals, the judiciary has come up with the above discussed legislations.

REFERENCES:

[1] Anderson, T. M. & Gardener, T.J. (2015). *Criminal Law: Twelfth Edition.* Stanford, CT: Cengage Learning

[2] Bar Association of India (2015). *Anti-Bullying Laws in India.* Retrieved from https://www.indianbarassociation.org/wp-content/uploads/2015/11/Anti-bullying-laws-in-india.pdf

[3] Brenner, W. Susan (2010). *Cybercrime: Criminal threats from cyber space.* Green Wood Publishing Group, Westport.

[4] Chinov, Mike (2000). *Aid Workers Decry Growing Child Sex Trade in Cambodia.* CNN.com Retrieved from http://archives.cnn.com/2000/asianow/southeast/09/18/cambodia.pedophile/index.html

[5] Staff Author, CNN (2001). *Sex Slavery: The Growing Trade.* CNN.com Retrieved from https://archives.cnn.com/2001/world/europe/03/08/women.trafficking/

[6] Flemming, P. and Stohl, M. (2000). Myths and Realities of Cyber terrorism. *International Conference on Countering Terrorism through Enhanced International Cooperation,* Page No. 22-24, September, Italy.

[7] Hafele, D. M. (2004). Three different shades of Ethical Hacking: Black, White and Grey. February 23, 2004.

[8] Higgins, George (2010). *Cybercrime: An Introduction to an Emerging Phenomenon.* Mc Graw Hill Publishing, New York.

[9] Holt, Thomas J. (2011). *Crime Online: Correlates Causes and Contexts.* Caroline Academic press, USA.

[10] International Journal of Social Science and Humanities Research (2016). *A Sociological Study of Different Types of Cyber Crimes.* Vol.4, Oct-Dec 2016. Retrieved from http://www.researchpublish.com/journal/IJSSHR/Issue-4-October-2016-December-2016/0

[11] Singh, Talwant (2011). *Cyber Law and Information technology.* New Delhi, India.

[12] Wall, David S. (2001). *Crime and the Internet.* Routledge, London.

[13] www.tigweb.org/actiontools/projects/download/4926.docx

[14] http://www.interpol.int/public/technologycrime/crimeprev/itsecurity.asp#21/4/2015

[15] https://www.tutorialspoint.com/information_security_cyber_law/introduvtion.htm

[16] https://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india

[17] http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW

[18] http://deity.gov.in/sites/upload_files/di/files/downoads/itact2000/itbill2000.pdf

[19] http://www.lawyersclubindia.com/articles/Classifiaction_Of_CyberCrimes_1484.asp

[20] http://vikaspedia.in/education/Digital%20Literacy/information-security/cyber-laws

[21] https://www.ijarcsse.com/docs/papers/Volume_5/8_August2015/V518-0156.pdf

[22] https://indiankanoon.org/doc/1439440/

[23] http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20%202008%20%28amendment%29.pdf

[24] https://cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/