Page 796 - 807 **DOI:** *https://doij.org/10.10000/IJLMH.113647*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 5

2022

Cyber Crimes and Legal Involvements of 5g Technology in India

KOMALA SANTOSH KUMAR[1] AND K. ANOUSHIKA[2]

ABSTRACT

The Paper discusses the understanding of cybercrime and legal involvements in India. The Internet, the worldwide connection of loosely held networks, has made the float of information and information among unique networks easier. With data and information being transferred among networks at remote places, security issues have become a prime subject over the past few years. Few people have additionally used the internet for crook activities like unauthorised access to other networks, scams, etc. these criminal activities associated with the internet are termed Cyber Crimes. With the increasing reputation of online activities like online banking, online shopping, and so on., it's far a period that we regularly listen to information. Therefore, a good way to stop and punish cyber criminals, "Cyber regulation", was introduced. Cyber regulation can be described as the law of the internet, i.e., it's far part of the legal systems that deal with the internet, cyberspace and other legal issues like online security or privacy.

Keywords: *Cybercrime, Legal involvements, Cyber regulations, Hackers, Hacking, Cyber Terrorism, Cyber theft.*

I. INTRODUCTION

A computer is defined as a machine that stores and processes information which the user directs. Technology like the internet has made it possible for data to flow through different networks easier and effectively. Internet technology is used for various purposes, from online dealings to online transactions. Over time, many computer users have been using a computer for personal or professional purposes. As such, security-related issues have become a major concern for administrators. This has given birth to "Cyber Crimes", or crimes committed over computers, usually over the Internet. A cybercrime can thus be defined as any crime where an offender must use a device or computer network to commit their offence. Unlike traditional crimes which happen in the physical world that involve meeting locals on the street, cybercriminals usually occupy themselves with hacking private documents or accounts without permission; divulging confidential business data without permission, or disabling devices without permission. Other

[1] Author is an Advocate at High Court of Telangana, India.
[2] Author is a CSE Student at Stanley College of Engineering and Technology for Women, Hyderabad, India.

 [ISSN 2581-5369]

offences that constitute cybercrime include accessing someone else's private data without permission, theft of intellectual property such as software; selling someone else's data without consent from the owner; and downloading illegal content from sources like torrent sites.

Cybercrime is a growing problem that has caused many damages to individuals, organisations and government agencies. Cyberlaw was introduced in India to prevent these crimes. The UN's General Assembly recommended India's first Information Technology (IT) Act in 2000. This Act was passed on the "United Nations Model Law on Electronic Commerce (UNCITRAL) Model".

The 5G services were being tested on a local Indian platform by the DoT in association with educational institutions like the Indian Institute of Technology (IIT) Bombay, IIT Delhi, IIT Hyderabad, IIT Madras, IIT Kanpur, and Indian Institute of Science (IISC) Bangalore. Other organisations like the Society for Applied Microwave Electronics Engineering & Research (SAMEER) and the Centre of Excellence in Wireless Technology (CEWiT) were also involved in the testing.

With this, the country aims to use small-cell technology for the 5G rollout. In small cell technology, the cells are installed in dense matter because of their short range. The density improves the geographical coverage. The Bhaskaracharya Institute of Space Applications and Geoinformatics (BISAG-N), located in Gujarat, has been helping the states in the mapping exercise.

What is cybercrime?

Sussman and Heuston were the first to propose the term "Cyber Crime" in 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] (UNODC, 2013). 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 cybercrime problems. Certain amendments were made to this Act in 2008, thereby passing the Information Technology (IT) Act, 2008, covering a wide range of areas 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]

 [ISSN 2581-5369]

Who are the Hackers and Crackers:

Hacker: 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 affects it injuriously by any means is a hacker.

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, steals information located on secure computers and causes disruption to the networks for personal or political motives.

II. CLASSIFICATION OF CYBER CRIMES:

Computer crimes exist in India and all over the world, often causing harm against governments, individuals or institutions. The common types of cybercrimes are discussed as follows:

1) Hacking

Hacking is a generic expression in the computing world and can be applied in many contexts. In strictly computing terms, a hack is a quick fix or clever solution to a restriction. 'hack' is temporary if an ingenious fix or 'make do' rather than an attack on a system. Tricking a machine into performing an unintended task is the predominant characteristic of a 'hack'; even well known simple tricks such as sticking sello-tape over pre-recorded audio or video tapes to enable reuse as a 'blank' tape can be described as 'hacks'.

In the popular and in legal mind, however, hacking has become unequivocally associated with the act of obtaining unauthorised access to programmes or data held on a computer system. This initial act is often followed by attempts to modify or delete the contents computer system. When, for example, the Communications Decency Act, which sought to impose controls over the content on Internet sites, was being debated in the United States legislature, hackers secured access to the Department of Justice's WWW pages and replaced the department's logo with a pornographic picture.

It simply refers to having an unauthorised access to another computer system. It is the most dangerous and commonly known cybercrime. The hackers break down the computer system and steal valuable information, known as data, from the system without permission. Hacking can be done for multiple purposes like data theft, fraud, destruction of data, and causing damage to a computer system for personal gains. Therefore, hackers are able to spoof the data and

 [ISSN 2581-5369]

duplicate the IP address illegally.

According to the research committed by the SANS Institute (2021), there are 10 different types of hackers:

1	**White Hat Hackers:**	"These are the ethical hackers that use their hacking skills for good reasons and do not harm the computer system."
2	**The Black Hat Hackers**	"These types of hackers use their computer knowledge to gain unauthorised access to a computer system with a malicious or harmful intention. They may steal, modify or erase data, insert viruses and damage the system."
3	**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]
4	**Script Kiddies**	"They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites."
5	**Green Hat Hackers**	"Green hat hackers are types of hackers who're learning the ropes of hacking. They are slightly different from the Script Kiddies due to their intention."
6	**Blue Hat Hackers**	"They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries."
7	**Red Hat Hackers**	"Red hat hackers are quite ruthless while dealing with black hat hackers or counteracting with malware. The red hat hackers continue to attack and may end up having to replace the entire system set up."
8	**State/Nation Sponsored Hackers**	"Government appoints hackers to gain information about other countries. These types of hackers are known as State/Nation sponsored hackers."
9	**Hacktivist**	"Hacktivists can be an individual or a bunch of nameless hackers whose intent is to gain access to government

 [ISSN 2581-5369]

		websites and networks. The data gained from government files accessed are used for personal political or social gain."
10	**Whistleblower**	"These types of hackers include individuals working in an organisation who can expose confidential information."

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

3) Cyber Warfare: It is an Internet-based conflict involving politically motivated computer system attacks. 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.

4) 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.

5) Domain Hijacking*:* It refers to the act of changing the registration of a domain name without the permission of its original registrant.

6) 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.

7) 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].

 [ISSN 2581-5369]

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.

8) 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 morphingor 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.

9) 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).

10) 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."
- Forgery: *"*It means making of false document, signature, currency, revenue stamp, etc."

11) 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**: Employees who have legitimate access to their company's computer can commit cyber crimes. These crimes often come about when an employee wants to make more money.

 [ISSN 2581-5369]

- **Corporate Espionage:** This types of crime typically targets any business and it's committed by someone from inside or outside the company. They may use the company's computers to steal important information like client lists, marketing strategies, personal data, and trade secrets..
- **Plagiarism:** Copymatic solves the problem of plagiarism by providing authentic content for your blog. It does this by using a combination of structured data and machine learning to create unique content, just like what a human would do. Copymatic doesn't contain any plagiarized content, signs of extensive usage of copy paste, or any real-time bots from major blog-nets.
- **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. It is very common now. This can be done by one of two techniques: changing the actual address in the email header and creating an email that looks like it emanates from another email account. The main idea behind this technique is to trick people into opening harmful attachments or clicking on links that may contain malware or scams.[11]
- **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.

III. IMPORTANCE OF 5G IN LAW ENFORCEMENT

- It will enhance efficiency, productivity, and security by helping the police access critical information in real-time and find criminals through high bandwidth and low latency.
- It ensure better performance in police devices such as body cams, facial recognition technology, automatic number-plate recognition, drones, and CCTVs.
- It will provide clearer images which will make it easier for Police by looking at hazy images from devices and attempting to interpret them.
- Police will be able to streamline their investigation methods due to the increased storage capacity promised by 5G.
- It will also allow rapid and secure communication within the organisation as well as between civilians and emergency responders.
- The police can access and analyse crime data and information from other infrastructure, such as traffic lights, from a remote location.

 [ISSN 2581-5369]

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. seven new Cyber Offences were added to ITAA, 2008 under the following sections:

S.No.	Sections under the IT Act, 2008 (Amendment)	Punishment
1.	**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.
2.	**Section 66C:** Identity Theft	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
3.	**Section 66D:** Phishing, i.e., punishment for cheating by personating 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.
4.	**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.
5.	**Section 66F:** Cyber Terrorism	Life imprisonment.
6.	**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.
7.	**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

 [ISSN 2581-5369]

		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:

S 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.

IV. UNDERSTANDING THE PREVENTIVE MEASURES

The solution to the problem of cybercrime depends on a number of factors. One should abide by the cyber law and also keep in mind that any new technology has some risk associated with it. Technology is changing at a rapid pace, and so are the means of committing crime. Hence, innovative measures are required to curb the issue of hi-tech crime. Apart from implementing stricter Laws, one must have knowledge about the best practices for protection against hacking and other cybercrimes. Such knowledge can be obtained through seminars conducted by

 [ISSN 2581-5369]

specific organizations or reading publications related to cyber security.

- Awareness need to be generated a few of the students on the grassroot stage, i.e., knowledge approximately cybercrimes and cyber laws. Cyber literacy should be given to the students in laptop centers, faculties, colleges and Universities as well. Cyber law attention programme may be prepared in any educational institute so that you can offer primary understanding of net and internet's safety.
- Keep your personal information safe by not sharing it with anyone
- 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.
- 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.
- Same passwords should not be kept for every online service you use. Keep different passwords for different online activities.
- 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.'
- 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.

V. 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. The deployment of 5G will be a game changer for law enforcement agencies. However, in order to implement 5G in India in the best possible way, government should create a national road map that takes into account law enforcement needs and adopt measures to hinder crimes facilitated by 5G technology.

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 for the victims and punish the criminals, the judiciary has come up with the above-discussed legislations.

*****

 [ISSN 2581-5369]

VI. REFERENCES

1. Cybercrime Definition, http://cybercrime.org.za/definition
2. Cyber Laws in India, http://cyberlawsinindia.net/black-html
3. The Jargon Dictionary on website, http://www.netmeg.net/jargon/terms/c/cracker.html
4. SANS Information Security White Papers, https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-grey-1390
5. Encyclopedia Britannica, https://www.britannica.com/EBchecked/topic/130595/Cyber crime
6. SANS, https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-grey-1390
7. You Dictionary: http://www.yourdictonary.com/cyberpornography
8. Cyber Crime Lawyers in Delhi, India, https://cybercrimelawyer.wordpress.com?category/66-c-punishment-for-identity-theft/
9. Email Spoofing: https://www.techopedia.com/definition/1664/email-spoofing
10. yber Crime Lawyers in Delhi, India, https://www.cyberlawsindia.net//cyber-india-html
11. Anderson, T. M. & Gardener, T.J. (2015). Criminal Law: Twelfth Edition. Stanford, CT: Cengage Learning
12. Brenner, W. Susan (2010). Cybercrime: Criminal threats from cyber space. Green Wood Publishing Group, Westport.
13. Hafele, D. M. (2004). Three different shades of Ethical Hacking: Black, White and Grey. February 23, 2004.
14. Higgins, George (2010). Cybercrime: An Introduction to an Emerging Phenomenon. Mc Graw Hill Publishing, New York.
15. Holt, Thomas J. (2011). Crime Online: Correlates Causes and Contexts. Caroline Academic press, USA
16. Varghese, Grace (2016). A Sociological Study of Different Types of Cyber Crime. *International Journal of Social Science and Humanities*,4(4), 599-607

*****

 [ISSN 2581-5369]