International Journal of Leading Research Publication
IJLRP

© IJLRP | ISSN (O) - 2582-8010
July 2021 | Vol. 2 Issue. 1
www.ijlrp.com

Cyber Laws & Cyber Crimes in India

Dr. Surender Kumar

LLM. Ph.D., Principal Shaheed Bhagat Singh Law College, Hanumangarh

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.

Keyword: *Cyber, Laws, Crimes, Worldwide, Computer, Cyberspace, Hackers*

1. 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".

2. OBJECTIVES

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

I. 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;

II. Generate awareness among the masses on "Cyber laws" that are imposed in order to stop the cybercrime and/or punish the cyber criminals; and

© IJLRP | ISSN (O) - 2582-8010
July 2021 | Vol. 2 Issue. 1
www.ijlrp.com

III. To suggest other preventive measures apart from the Cyber Law so that there can be safety of the users in the cyberspace.

3. 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 orsystems1. 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, 2008covering 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.

4. THE PERPETRATORS-HACKERS AND CRACKERS

Hacker: According to Section 66A of Information Technology (IT) Act, 20003, 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

Crackers: According to the Jargon Dictionary4, 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.

5. 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:

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:

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. Black Had 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.
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.

CYBER TERRORISM:

It refers to unlawful attacks against computers, networks and the information stored therein that are carried out to intermediates 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. The cyber terrorism attacks and threats include:

1. **Cyber warfare:** It is and 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.
2. **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.
3. **Domain Hijacking:** It refers to the act of changing the registration of a domain name without the permission of its original registrant.

© IJLRP | ISSN (O) - 2582-8010
July 2021 | Vol. 2 Issue. 1
www.ijlrp.com

CYBER STALKING:

It is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. It is a wilful conduct by the cyber stalkers through any online medium like email, social media, chat rooms, 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.

CYBER BULLYING:

According to the Oxford Dictionary, 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 delinquency8. 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

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. 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 cyber sex 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).

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, 200810.

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.

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 attackers ends 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.