# INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

# [ISSN 2581-9453]

**Volume 2 | Issue 3**

**2020**

# Cyber Crime and Law

**SHALABH**[1]

## ABSTRACT

*Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.*

*Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:*

- *Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.*
- *Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.*

*The FBI identifies cybercrime fugitives who have allegedly committed bank fraud and trafficked counterfeit devices that access personal electronic information. The FBI also provides information on how to report cybercrimes, as well as useful intelligence information about the latest cybercriminals.*

*This paper highlights the kinds of law made for the cyber-crime also how effective the laws are, along with the loopholes and types of development required in this sphere.*

## I. INTRODUCTION

In technically driven society, people use various devices to make life simple. Globalization results in connecting people all around the world. The increasing access to and continuous use of technology has radically impacted the way in which people communicate and conduct their

[1] Author is a Practicing Advocate in India.

 [ISSN 2581-9453]

daily lives. The internet connects people and companies from opposite sides of the world fast, easily, and relatively economically. Nevertheless, the internet and computer can pose some threats which can have disparaging impact on civilisations. Cybercrime is a hazard against different organisations and people whose computers are connected to the internet and particularly mobile technology.

Cybercrime is a dangerous crime involving computers or digital devices, in which a computer can be either a target of the crime, a tool of the crime or contain evidence of the crime. Cybercrime basically defined as any criminal activity that occurs over the Internet. There are many examples such as fraud, malware such as viruses, identity theft and cyber stalking. In present environment, since most information processing depends on the use of information technology, the control, prevention and investigation of cyber activities is vital to the success of the Organizations, Government's agencies and individuals. The procurement and maintenance of highly skill cybercrime expert by Government and Business Enterprises cannot be exaggerated.

Earlier, cybercrime was committed mainly by individuals or small groups. Presently, it is observed that there are highly complex cybercriminal networks bring together individuals at global level in real time to commit crimes.

Today, criminals that indulge in cybercrimes are not motivated by ego or expertise. Instead, they want to use their knowledge to gain profits promptly. They are using their capability to snip, deceive and exploit people as they find it easy to generate money without having to do an honest work. Cybercrimes have become major threat today.

Cybercrimes are broadly categorized into three groups such as crime against

1. Individual
2. Property
3. Government

**1. Individual:**

This type of cybercrime can be in the form of cyber stalking, distributing, trafficking and "grooming". In present situation, law enforcement agencies are considering such cybercrime very serious and are joining forces worldwide to reach and arrest the committers.

**2. Property:**

Same as in the real world where a criminal can steal and pickpocket, even in the cyber world, offenders' resort to stealing and robbing. In this case, they can steal a person's bank details and

drain off money; misuse the credit card to make frequent purchases online; run a scam to get naive people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

3. **Government:**

Crimes against a government are denoted to as cyber terrorism. If criminals are successful, it can cause devastation and panic amongst the citizen. In this class, criminals hack government websites, military websites or circulate propaganda. The committers can be terrorist outfits or unfriendly governments of other nations.

## II. TYPES OF CYBER CRIME

**There are many types of cybercrimes:**

**Hacking:**

In this category, a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is categorized as a wrongdoing and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location. Many crackers also try to gain access to resources through the use of password cracking soft wares. Hackers can also monitor what users do on their computer and can also import files on their computer. A hacker could install several programs on to their system without their knowledge. Such programs could also be used to steal personal information such as passwords and credit card information.

**Theft:**

This type of cybercrime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Nowadays, the justice system is addressing this cybercrime and there are laws that avert people from unlawful downloading.

**Cyber Stalking:**

This is a type of online harassment wherein the victim is endangered to a barrage of online messages and emails. Normally, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not

having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more dejected.

**Identity Theft:**

This is a major problem with people using the Internet for cash transactions and banking services. In this cybercrime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card, full name and other sensitive information to drain off money or to buy things online in the victim's name. The identity thief can use person's information to fraudulently apply for credit, file taxes, or get medical services. It can result in major financial losses for the victim and even spoil the victim's credit history.

**Malicious Software:**

This software, also called computer virus is Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to gather sensitive information or data or causing damage to software present in the system.

**Child soliciting and Abuse:**

This is also a type of cybercrime in which criminals solicit minors via chat rooms for the purpose of child P.graphy. The FBI has been spending a lot of time monitoring chat rooms visited by children in order to reduce and prevent child abuse and soliciting.

Virus dissemination: Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, web jacking, e-mail bombing etc.).

**Computer vandalism:**

It is a type of cybercrime that Damages or destroys data rather than stealing. It transmits virus.

Cyber terrorism: It is a use of Internet based attacks in terrorist activities. Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt.

## III. BACKGROUND

The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage’s analytical engine is considered as the time of present-day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened and prefer to sabotage so as to discourage

Jacquard so that the new technology cannot be utilized in the future.

## IV. SAFETY IN CYBERSPACE

Lists are some points, one should keep in mind while surfing the internet:

- If possible always use a strong password and enable 2 steps or Two-step authentication in the webmail. It is very important in order to make your webmail or your social media account secured. Guideline of strong password:

¬Password should be of minimum eight characters.

¬One or more than one of lower case letter, upper case letter, number, and symbol should be included.

¬Replace the alike character. Example- instead of O we can use 0, instead of lower case l we can use I etc. Example of strong password: HelL0 (%there %); Thing need to avoid while setting the password: ¬Never use a simple password that can easily be decrypt Example- password ¬Personal information should never set as a password. ¬Repeating characters should be avoided. Example- aaaacc ¬Using of same password in multiple sites should be avoided. What is 2 step or Two-step authentication? This is an additional layer of security that requires your user name and the password also a verification code that is sent via SMS to the registered phone number. A hacker may crack your password but without the temporary and unique verification code should not be able to access your account.

- Never share your password to anyone.
- Never send or share any personal information like bank account number, ATM pin, password etc over an unencrypted connection including unencrypted mail. Websites that doesn't have the lock icon and https on the address bar of the browser are the unencrypted site. The "s" stands for secure and it indicates that the website is secure.
- Don't sign to any social networking site until and unless one is not old enough.
- Don't forget to update the operating system.
- Firewalls, anti- virus and anti-spyware software should be installed in ones PC and should be regularly updated.
- Visiting to un-trusted website or following a link send by an unknown or by an un-trusted site should be avoided.
- Don't respond to spam.
- Make sure while storing sensitive data in the cloud is encrypted.

- Try to avoid pop-ups: Pop-ups sometimes comes with malicious software. When we accept or follow the popups a download is performed in the background and that downloaded file contains the malware or malicious software. This is called drive-by download. Ignore the pop-ups that offer site survey on ecommerce sites or similar things as they may contain the malicious code.

## V. CYBER LAW

Cyber Law took birth in order to take control over the crimes committed through the internet or the cyberspace or through the uses of computer resources. Description of the lawful issues that are related to the uses of communication or computer technology can be termed as Cyber Law. What is the importance of Cyber Law? Cyber law plays a very important role in this new epoch of technology. 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, but each action and each reaction in Cyberspace has some legal and Cyber legal views. Cyber Law awareness program Once should have the following knowledge in order to stay aware about the cyber-crime:

- One should read the cyber law thoroughly.
- Basic knowledge of Internet and Internet's security.
- Read cyber crime's cases. By reading those cases one can be aware from such crimes.
- Trusted application from trusted site can be used for protection of one's sensitive information or data.
- Technology's impact on crime. The Information Technology Act of India, 2000 According to Wikipedia "The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cybercrimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997". 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.
- 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 be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company. Cyber Law in India Following are the sections under IT Act, 2000

1. **Section 65-** Temping with the computers source documents Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network.

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

**2. Section 66-** Hacking with computer system, data alteration etc.

Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking.

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both

**3. Section 66A**- Sending offensive messages through any communication services

- Any information or message sent through any communication services this is offensive or has threatening characters.
- Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will.
- Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages. Punishment: Any individual found to commit such crimes under this section could be sentenced upto 3years of imprisonment along with a fine.

**4. Section 66B-** Receiving stolen computer's resources or communication devices dishonestly Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the reason to believe the same.

Punishment: Any person who involves in such crimes could be sentenced either description for

a term that may extend upto 3 years of imprisonment or with a fine of rupee 1 lakh or both.

**5. Section 66C-** Identify theft Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime.

Punishment: Any person who involve in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

**6. Section 66D-** Cheating by personation by the use of computer's resources Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

**7. Section 66E-** Privacy or violation Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.

**8. Section 66F-** Cyber terrorism A. Whoever intentionally threatened the integrity, unity, sovereignty or security or strike terror among the people or among any group of people byI. Deny to any people to access computer's resources. II. Attempting to break in or access a computer resource without any authorization or to exceed authorized access. III. Introducing any computer's contaminant, and through such conducts causes or is probable to cause any death or injury to any individual or damage or any destruction of properties or disrupt or it is known that by such conduct it is probable to cause damage or disruptions of supply or services that are essential to the life of people or unfavorably affect the critical information's infrastructure specified under the section 70 of the IT Act. B. By intention or by knowingly tries to go through or tries to gain access to computer's resources without the authorization or exceeding authorized access, and by such conducts obtains access to the data, information or computer's database which is limited or restricted for certain reason because of the security of the state or foreign relations, or any restricted database, data or any information with the reason to believe that those data or information or the computer's database obtained may use to cause or probably use to cause injury to the interest of the independence and integrity of our country India.

Punishment: Whoever conspires or commits such cyber crime or cyber terrorism shall be sentenced to life time imprisonment.

**9. Section 67-** Transmitting or publishing obscene materials in electronic form Whoever

transmits or publishes or cause to publish any obscene materials in electronics form. Any material that is vulgar or appeal to be lubricious or if its effect is for instance to tends to corrupt any individual who are likely to have regard to all relevant circumstances to read or to see or to hear the matter that contained in it, shall be sentenced on the first convict with either description for a term that may extend upto five years of imprisonment along with a fine which may extend upto 1 lakh rupee and in the second or subsequent convict it can be sentenced either description for a term that may extend upto ten years along with a fine that may perhaps extend to two lakhs rupees.

## VI. CONCLUSIONS

The rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent years. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cybercrimes. The Act further revise the IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act 1891 and the Reserve Bank of India Act, 1934. Any part of the world cyber-crime could be originated passing national boundaries over the internet creating both technical and legal complexities of investigating and prosecuting these crimes. The international harmonizing efforts, coordination and co-operation among various nations are required to act towards the cyber-crimes. Our main purpose of writing this paper is to spread the content of cyber-crime among the common people. At the end of this paper “A brief study on Cyber Crime and Cyber Laws of India” we want to say cyber-crimes can never be acknowledged. If anyone falls in the prey of cyber-attack, please come forward and register a case in your nearest police station. If the criminals won’t get punishment for their deed, they will never stop.

****

 [ISSN 2581-9453]