Cyber Crime in India: Problem and Law related to Cyber Crime

AUTHOR 1: TUNICHA KONSAM,
FIFTH YEAR, B.A.LLB.,
LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY
AUTHOR 2: DR. SANDHYA VERMA
ASSISTANT PROFESSOR,
LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY

Abstract*: Today's generation of world is a cyber world; we cannot live without the use of internet not only the adult but also the children. There is no doubt and we cannot deny that internet is helping every living person. And on top of this it is a great help during the pandemic, because due to lockdown (covid-19) schools, colleges and other work place had to shut down all around the world. This has affected 1.2 billion children in 186 countries. Thanks to this digital platform, it turns out more helpful for children and workers. But as easy access and wide spread of online community becomes the criminal also fine its way to get through for new easy way of crime to commit and this is the prove and result of rising cybercrime. This article emphasizes the problem created by cybercrime towards individual or group in society and how to deal with this type of crime by studying a little detail about cyber law in India perspective. And about the definition of cyber crime there is no fixed definition for cybercrime. The Indian Law has not given any definition to the term 'cybercrime'. In fact, the Indian Penal Code does not use the term 'cybercrime' at any point even after its amendment by the Information Technology (Amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.*

Keyword: Cyber crime, Internet, Criminal, Network, Cyber space, Cyber law, Punish.

Introduction

In today's world crime rate are increasing day by day. There is no place without crime in the world, small or big, whether physically present or not, every type of crime and criminal exist in this world. But why does such crime exist? Why people try to commit crime even when they know the consequence? Why ready to risk their life? Why ready to risk their life for someone else?

All this exist in everyone's mind throughout history and the most common thing for crime to happen in this world is because of one's own greed, anger, jealousy, revenge, pride or insecurity. Some even commit crime with well plan just to have less risk and gain what they wanted to. These kinds of people choose their own behavior and attitude. They think that life of a crime is better than a regular job. People find shortcut that is the most sadness part of our reality.

As we already know Crime has been a big issue of this world and has many types but in this topic we will focus on "CYBER CRIME" on Indian scenario, its problem and law related to it.

Social media is a very important part of our life. In today's world people depend more on internet we can also say cyber world or cyberspace. It is a medium of communication, information, commerce, entertainment, research work or payment, all of this now available on internet is making it very easy for living and helpful. But as we know every good impact there is bad impact, if positive there is negative. So, as social media is no doubt very useful to one's own life but it is also destroying many people life. Just like internet making it easy for people, it is also making it easy for criminal to commit crime, this crime is known as "Cyber Crime".

"Cyber Crime" is a crime when a criminal targets other internet users through computers or other information technology, who have ill intention towards any particular individuals, parties or groups. But most of people believe Cyber Crime is just a criminal activity which hackers steal other people's financial information but that is not the only thing about cybercrime. As we know that, now internet usage has increase drastically in the last few years, and that have help evolving new threats and criminal in cyber world.

Definition of Cyber Crime

In Simple way we can say that cyber crime is an unlawful act in which computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code (IPC). The abuse of computers has also given birth to areas of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways:-

- The Computer as a Target: - using a computer to attack other computers. E.g. Hacking, Virus/Worm attacks, DOS attack etc.
- Computer as a weapon: - using a computer to commit real world crimes. E.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

There isn't really a fixed definition for cybercrime. The Indian Law has not given any definition to the term 'cybercrime'. In fact, the Indian Penal Code does not use the term 'cybercrime' at any point even after its amendment by the Information Technology (Amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Cyber Crime is not defined officially in the IT Act or in any other legislation. In fact, it cannot be too. Offense or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and related legislation. Hence, the concept of cybercrime is just a "combination of crime and computer".

The Most Common Type of Crime in Cyber Crime

There are many type of Cyber Crime and also as the technology keeps rising, the different types of cyber crime increase. New technology means adding a new type of cyber crime because if there is a developer there is a destroyer or to misused of the new technology. There are some common cyber crimes in India with the punishment given below:-

- **Hacking**
  Hacking is the most common crime in the world of cyber space. It is gaining unauthorized access to your system profit, protest, information gathering or to evaluate system weakness. The provisions for hacking are given in IT Act, 2000 under section 43-A and 66 and section 379 & 406 of Indian Penal Code (IPC). The punishment of hacking is 3 years or shall be imposed with fine up to 5 lakh.

- **Denial of Service (DOS)**
  Denial of Service attack is an attack to computer that brings down any server making it inaccessible to intended users. It is known as the flooding machine with requests in an attempt to overload systems, target with traffic or sending it information that triggers a crash. It also uses bots for tasks. The provisions are given under section 43(f) of IT Act, 2000 with imprisonment up to 3 years or with fine up to 5 lakh rupees.

- **Virus Dissemination**
  Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. Virus Dissemination involves direct or search unauthorized access to system by introducing malicious programs known as viruses, worms etc. Virus needs host while worms are standalone. Provisions are provided under the IT Act, 2000 under sections 43-C, 66 and section 268 of the Indian Penal Code (IPC).

- **Credit Card Fraud**
  Credit Card is a plastic card that represents the line of credit. It allows the cardholder to buy goods and services on credit based on the cardholder's promise to pay back the money. Globalization and increased use of the internet for online shopping have led to excessive use of credit cards. Card fraud begins either with the theft of the physical card or with comprise of data associated with the account. Provisions of such fraud are given under section 66 C and 66 D of IT Act, 2000 and section 468 & 471 of Indian Penal Code, 1860.

- **Phishing**
  Phishing is a malicious individual or group who scam users. They do so by sending e-mail or creating web pages that are designed to collect an individual's online bank credit card or

other login information. The provisions to prosecute any person for phishing are given under section 66 C, 66 D and 74 of the IT Act with imprisonment up to 3 years or with fine up to 1 lakh.

- **Cyber Stalking**
  Cyber Stalking can be define as the use of electronic communications to harass or frighten someone, for example by sending threatening email, massages or picture. The provisions are given under IT Act, 2008 under section 72 and section 354 C (voyeurism) of the Indian Penal Code. Also section 67 provides imprisonment up to 3 years with fine.

Problem that lead to the commission Cyber Crime

Cyber crime is an illegal activity carried out using technology where a computer is the object of the crime; it is used as a tool to commit an offense. As the Internet of Thing (IOT) evolves and smart devices become more popular, cyber criminals have increased opportunities to get into security measures, gain unauthorized access and commit crime. Cyber crime adds up to countless costs in damages every year, impacting individuals, businesses and even government. Unlike crimes are committed in the physical world, cyber crime requires little to no investment to be carried out. Cyber criminals have easy way to make big money and target organization like bank, casinos and financial firms where a huge amount of money flows daily and hack sensitive information. Things that lead to this problem of cyber crime is:-

- **Breach because of Mobile Devices**
  In 2015, mobile devices had less than 1% infection rate, so they were considered safe. Now more than 3/5 of IT security professional report that it is either certain. Since the rise and development of smartphone cyber crime has become more easy access for the cyber criminals. Number of attacks against mobile phones has increased by over 50% in the first half of 2019, as compared to the same period in 2018. Check point mobile security report 2021 says 4/10 mobiles are vulnerable to cyber attacks, 97% of organization globally in 2020 face mobile threats that use multiple attack.
- **Embedding Malware into Legitimate Application**
  Cyber criminals have embedded malware into legitimate applications and they are targeting poorly secured WiFi spots, stealing passwords and more in their quest to steal information.
- **Exploiting Unauthorized Products**
  In many cases, attackers like to exploit unauthorized products having weak security controls in the corporate cloud. So, it is very important to keep strong security for all individuals system.
- **Unlimited Internet Access**
  Unlimited of internet is the major factor of cyber crime towards individuals. We have given convenience in accessing without any limitations. Example like nowadays many telecom brands have involve, new are formed and in the market they have their own competition which made them create such unlimited and given more facilities for customers. This give easy access and even for kids.

- **Lack of Awareness**
  Human errors in cyber security still a leading cause of many if not most data breaches. There is lack of awareness in people who are at the receiving end of the scams. Most people tend to open phishing emails and hence they put in a situation which there is danger of loss, harm for their personal information.

Law regarding Cyber Crime in India

Cyber Law in India

When internet was developed, there was hardly any thought of internet could transform into tool/weapon to be misuse by the criminals. But today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence this is the reason of need for Cyber laws in India. Which arise of passing the bill of Information technology?

IT Act, 2000

In order to prevent Cyber crime in India, in 2000, both the house of Indian parliament passed Information Technology Bill. After the bill received the assent of the president in August 2000, it came to known as Information Technology Act, 2000. Cyber Law is contained in the IT Act, 2000. The aims of this Act:-

- Is to provide the legal infrastructure for e-commerce in India. Cyber laws have a major impact for e-businesses and the new economy in India.
- It also to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

Most of law regarding Cyber Crime is given under the IT Act of 2000 and (IPC) Indian Penal Code:

Cyber Crime under IT Act, 2000 -

- **Section 65, Tampering with computer source documents**
  Whoever knowingly or intentionally conceals, destroys or alters any computer source code (such as programmes, computer commands or design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years imprisonment or with fine of INR 2lakh or with both.
- **Section 66, Hacking computer system and data alteration**
  If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or a fine of INR 1lakh.

- **Section 67, Publishing Obscene Information**
  Whoever publishes or transmits or cause to be published in the electronic form or any material which is lascivious or appeal prurient interest shall be punished on first conviction with imprisonment which may be extent to 3 years with fine that can be extent to INR 5 lakh. On second conviction, imprisonment extent to 5 years and fine that extent to INR 10 lakh.
- **Section 70, Unauthorized Access of Protected System**
  The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Person who access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to 10 years and shall also be liable to fine.
- **Section 72, Breach of Confidentiality and Privacy**
  Penalty for breach of confidentiality and privacy: - Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to INR 1 lakh, or with both.

Cyber Crime under Indian Penal Code (IPC)

- **Section 420, Bogus Websites & Cyber Fraud**
  Whoever cheats and thereby dishonestly induces the person deceived any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
- **Section 463, Forgery of Electronic Records**
  Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.
- **Section 499, Sending Defamatory Message read with section 500, punishment**
  Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.
  And under section 500 say person who defames another shall be punished with simple imprisonment for a term which may extend to 2 years, or with fine, or with both.

- **Section 503, Sending Threaten Messages by Email**
  Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

There are also laws for Cyber Crime under Special Act, which include:-

- **Online Sale of Arms under Arms Act, 1959**
- **Online Sale of Drug under Narcotic Drugs and Psychotropic Substances Act, 1985**

Conclusion

Since the internet user are increasing day by day in the world, where everything related to technology is easy way to access someone information and can be taken out in few second, and criminal finding its easy way to commit crime have made the internet worldwide user at risk. Very useful technology is now a place for easy misuse as weapon to attack people. Thus cyber crime has become a threat to the mankind. In order to protect this Government took up the step to protect the people by passing bill of Information Technology Act, 2000 and by giving punishment under Indian Penal Code 1860. It also involved cyber crime under special Act like (i) online sale of arms under arms Act, 1959 and (ii) online sale of drugs under narcotic drugs and Psychotropic substances Act, 1985. And further more amendment for cyber law in order to help and aware the public from cyber attack.

Reference

- https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics
- https://www.tutorialsmate.com/2020/09/what-is-cybercrime.html
- https://www.britannica.com/topic/cybercrime
- https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime
- https://www.infosecawareness.in/cyber-laws-of-india
- https://www.lawctopus.com/academike/offences-act-2000/#:~:text=Cybercrime%20in%20a%20broader%20sense,a%20computer%20system%20or%20network.
- Halder, D & Jaishankar, K (2011) Cyber Crime and the Victimization of Women: Laws, Right and Regulations. Hershey, PA, USA: IGI Global.
- www.Legalserviceindia.com/legal/article-2019-importance-of-cyber-law-in-india.html
- www.legalserviceindia.com/legal/article-3042--types-of-cyber-crime-and-its-causes.html
- https://www.gadgets.ndtv.com/mobiles/news/check-point-mobile-security-report-2021-four-out-of-10-mobiles-vulnerable-cyberattacks-2413419
- www.lifars.com/2020/04/d0-you-know-why-cyber-crime-happens/
- https://www.yourstory.com/mystory/smartphones-prime-targets-cybercriminals/amp

- https://www.upcounsel.com/cyber-law
- https://www.cyberlawsindia.net/Information-technology-act-of-india.html
- http://www.bareactslive.com/ACA/ACT632.HTM