IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CYBER LAW and CYBER CRIME – A COMPREHENSIVE STUDY

Rudranil Bhandari
LLM student, ICFAI Law School,
The ICFAI University, Dehradun

ABSTRACT:

"*Cyber security is no longer just an IT issue, but the responsibility of every individual to ensure trust in this digital world.*" - Stephane Nappo

Cyber Law includes the rules and regulations about computer technology, the internet and digital communications. It deals with many things like data privacy, data protection, intellectual property rights, cyber security, cybercrime, online transactions etc.

On the other hand,cybercrime refers to illegal activities which involve computer networks, the internet and computers. Data theft, fraud,online harassment,hacking and spreading malicious software are part of Cybercrime which is committed through digital means. The criminal uses DVD, Pen Drives, Flash Drives, Micro Chip etc. The main issue is the crime takes a horrible face, particularly those, copyright infringement, child pornography so on.

The study includes various types of Cybercrimes including hacking, fishing, cyber stalking, online harassment, malware attacks, cyber fraud, cyber terrorism and more. This also highlights the challenges of cybercrime, its jurisdictions, rapid technology change, evidence collection and prevention etc.

It also explores the legal and regulatory measures whichhave been implemented by the government and international organizations regarding Cybercrime. This includes National Cyber security strategies, cybercrime laws, data protection and privacy regulations, and international corporation frameworks.

Keywords: Privacy, Protection, Cybercrime, Data Theft, Hacking, Technology.

1. INTRODUCTION

"*The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life.*" - Bill Gates

In this digital era, technologies and the internet changed the human lifestyle, from education, communication, entertainment and so on. Usage of the internet, technologies, human lifestyle become easier than past. Today the whole world is connected with the huge amount of data and the information which is constantly moving through

technology and electronic means. While this technology made many things easier and convenient, it has also led to a crime, called cybercrime. Because of sharing huge amounts of data in cyberspace, the scope of data breach or privacy breachbecomes a part of cybercrime. The cyber criminals mainly targeted individuals or companies to gain money and harm people.

As technology and digital systems grow, there is a need for legal frameworks and strategies to deal with cyber threats. Cybercrime can take many forms such as data theft, fraud, malware attacks, phishing, which are made to disrupt or damage computers.

The borderless nature of the internet or cyberspace made cybercrime a global issue in national boundaries, posing challenges for law enforcement agencies, and legal professionals. Due to the rapid evolution of technologies, it is very difficult to identify the proper jurisdiction.

The government and international organizations developed many legal and regulatory measures to control cybercrime, Cyber security strategies, cyber laws, data protection and data privacy regulations. The law enforcement agencies play a vital role investigating cybercrimes, conducting digital forensic promoting cyber security awareness etc. This comprehensive study targets to provide in death exploration of the cyber law and cybercrime including the types of challenges and the various legal and regulatory measures.

1.1. DEFINING CYBER LAW:

The internet and cyberspace related law is known as cyber law that includes the legal issues, regulations. Cyber law governs the usage of computer technology, the internet, and communication. Cyber law covers the areas of intellectual property rights, data privacy, data protection, online transactions, e-contacts, cyber security and the prevention of cybercrime.

Cyber law providesa legal framework regardingcrime, challenges that arise in the digital age. The aim of cyber law is to protect individuals, businesses and society from cyber-attacks or cyber thread and enabling the responsible usage of technology.

1.1.1. THE ROLE OF CYBER LAW:

- Data privacy and protection laws providesafeguardsforpersonaldata or information.
- Cyber law ensuresthe proper usage of data handling practices.
- Cyber law regulates the area of e-commerce, e-contracts, and online financial transactions etc.
- Under cyber law, an Intellectual property right protects digital content like software, music, videos etc.
- Cyber laws help to identify illegal online activities like hacking, cyber-stalking, fraud and provide safeguardsto the people from these.

1.2. DEFINING CYBER CRIME

Cybercrime is a type of crime where the involvement of a computer and a network are necessary. The computer system and the network may use as a toolin the crimes like, hacking malware attack, phishing, cyber stalking, online

fraud, cyber terrorism child pornography etc. Cyber criminals use the computer technology to get personal or sensitive data for the malicious purposes. They use computers for communication and data storage.

The criminals use cybercrime to get huge amounts of data, money or harm people. Some time it gets bigger like cyber terrorism, which is very dangerous to the society or community.

Nature of cyber crime

Cyber crime is a complex and evolving concept its nature can be broadly because of its boundary less nature. Cyber crime activities are carried out through the use of computers or computers networks and digital technologies. The nature of cyber crime can be classified into few points there –

- Cyber crime is intangible in nature.
- It is totally based on e-platform and technology, mainly virtual concept
- It has no geographical boundaries so it has borderless nature
- The constant advancement of technology continuously presents new opportunities for cyber criminals, rapid evolution is the another nature of the cyber crime

1.2.1. TYPES OF CYBERCRIME:

Cybercrimes is a broader term to define crimes; there are many types of crime thatcome under cybercrime. They are-

- **Hacking:** hacking is like unauthorized access to the computer system or network to steal data or information or cause damage. In simple terms it means an illegal intrusion into a computer system or network. There is a term of hacking known as cracking, but from Indian legal scenario there is no difference between hacking and cracking[1]. Every act committed towards breaking into a computer or network systemis called hacking. Hackers mainly use computer programs to attack the target computer. Some hackers hack for monetary gains, by stealing credit card information or transferring money from victim's bank accounts to their own.
- **Data Theft:** Data Theft is a type of crime where the criminal steal individuals personal or valuable data by accessing their computer, mobile phones, digital camera, e-mail, web page and so on. Nowadays cyber criminals use data theft process to threat or monetary gain. This kind of crime is easy for the office workers who have access to technology such as desktop computers, capable of storing digital information such as flash drives, iPods, digital cameras and even Mobile Phones.

In other words, if any person without permission of the owner, who oversees a computer or computer system - downloads, copies or extracts any dataor information from such computeris data theft.[2]

- **Social Engineering and Phishing:** it is a technique by which criminals manipulate people into doing things which they should not do like sharing information, but they share. Phishing is the technique of social engineering cybercrime.

[1]https://crimebranchjkpolice.nic.in/cybercrime.html
[2]Section 43 (b) of Information Technology (Amendment) Act, 2000

Phishing is an act of attempting to steal information such as usernames, passwords and credit card details by a trustworthy entity in electronic communication. Phishing is carried out from email spoofing, and it often directs users to enter details at a fake website which looks almost identical to the original one.

- **Cyberstalking:** it is a kind of stalking which is done through digital technologies to harass or threat individuals by using their data or information. Stalking is a kind of harassing or threatening behavior that an individual engages in repeatedly. It can be done using phone calls, written messages or vandalizing a person's property. Cyber stalking can be also defined as the repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using internet services.
- **Email Spoofing:** it is a very common technique whichis used in cybercrime.It is kind of an email-basedscam. When cyber criminals send emails to the victims as a different person or company or bank to gain their information.The purpose of email spoofing is to makepeople provide their sensitive information credit card details, bank details, or clicking on malicious linksthat can compromise their systems.
- **Malware attack:** it is a kind of virus or software which is distributed by cyber criminals to damage, gaininformation or disrupt computer systems.In all countries it is a serious criminal offence to create and distribute malware, but it continues to be produced for various reasons, such as demonstrating a capability or making money. Malware includes computer viruses, ransom ware, worms, Trojan horses, root kits, spyware, adware, malicious BHOs, rogue security software and other malicious programs which is very dangerous for Information technology.
- **Child Pornography:** Child pornography is a kind of pornography that involves child or child content. Pornography uses different types of media platform that includes magazines, photos, sculpture, drawing, cartoon, painting, animation, sound recording, film, video, and video games. Child pornography may be simulated child pornography or produced with the direct involvement of the child.

Legal definitions of child pornography generally include sexual images involving prepubescents, pubescent or post pubescent minors and computer-generated or AI-generated images that appear to involve them. Most of the possessors of child pornography are arrested because they have the possession of images of prepubescent children.

- **Cyber Terrorism:** it is another type of crime which is done by using digital technologies, such as computers, networks, and the internet to cause disruption, fear, and chaos in public or political objectives. It involves exploiting cyber systems and infrastructure to commitattacks that compromise crucial services, national security, and create panic among people. Cyber terrorists can be individuals or organized groups, target the infrastructure like financial systems and government agencies.

1.2.2. CHALLENGES IN COMBATING CYBERCRIME

Althoughthere are many laws whichdeal with cybercrimes, there should be changes in laws and regulation, because cybercrime changes or modify with the time and technology. There are various challenges in combating cybercrime. They are discussed below-

- **Jurisdictional Issues:** Cybercrime is a crime which is done in cyberspace, and it has no limitation or boundaries. It can be both national and international or global in nature because the internet is everywhere. So that it creates a big challenge to identify the jurisdiction of the crime.
- **Rapid Technological Evolution:** Technology is continuously evolving day by day with new technologies.The criminals use advanced technology to hide and secure their activities. The Laws and regulations must adapt by the time to control the Challenges.
- **Evidence Collection and storing:** Digital evidence is essential for the identification of the crime. The evidence, which iscollected or stored in digital means, can be easily modified, corrupted or destroyed. Collecting and storing evidence from computer systems is forensically admissible in court andrequires significant expertise.
- **Shortage of Expertise:** There are a very minimum number of professionals who are specialized incybersecurity, digital forensics and have skills needed to combat sophisticated cybercrimes. Training and recruiting professionals are the biggest challenge in this era is.
- **Public Awareness:** Many cybercrimes succeed by exploiting human vulnerabilities through hacking, phishing and social engineering. Raising public awareness about cyber threats and promoting better cyber practices can reduce crime.

1.3. Regulatory framework in India

India's National Cyber Security Policy dates back to 2013 and was created with the vision of building "a secure and resilient cyberspace for citizens, businesses and Government".1 The policy recognized the threats that cyber attacks carry, and the potential risks to human lives, the economy, and national security. The policy also identified key strategies for securing the cyberspace, most of which are applicable today. However, given that the policy is a decade old, a revised national policy for cyber security is well overdue. The Government had stated in December 2022 that it had formulated a draft cyber security strategy pertaining to the security of national cyberspace.2 However, the details of the strategy and timelines for implementation were not mentioned.

Information Technology Act, 2000 ("IT Act") The IT Act provides, inter alia, for punishment for offences committed relating to electronic communication or data, and other offences in relation cyber security. Certain offences such as access to computers, computer systems or computer networks without the permission of the owner/person in charge, downloading or copying data from computers and denial of access to computers also make the perpetrator liable to pay compensation

Computed related offences, Section 43[3] of the IT Act provides for compensation payable for certain actions in relation to computer infrastructure (i.e., computer, computer system, computer network) and computer resources when taken without the owner or person in charge of such computer infrastructure or resource. This includes unauthorized access, downloads, introduction of computer contaminants, damage, denial of access, among other acts. Under Section 66,

[3] Information Technology Act, 2000

these actions if done dishonestly or fraudulently are punishable with imprisonment up to 3 years, and / or a fine up to INR 500,000. Further, if any person has secured access to material containing personal information about another person, and discloses the same without the consent of the person, with the intent to cause or knowing that he is likely wrongful loss or wrongful gain, is punishable with imprisonment up to 3 years, and / or a fine up to INR 500,000

Tampering with computer source documents, The intentional concealment, destruction or alteration of computer source code when such source code is required to be kept or maintained under any applicable law is punishable with imprisonment of up to 3 years and/or with fine of up to INR 200,000

Dishonestly keeping stolen device/resource, a person who dishonestly keeps or receives any stolen electronic resource, knowing that such resource or device is stolen, may be punished with imprisonment of up to 3 years, and/or a fine of up to INR 100,000.

Identity theft**,** Identity theft involves fraudulent or dishonest use by a person of electronic signature, password or any other unique identification feature of another person. It is punishable with imprisonment up to 3 years, and a fine up to INR 500,000.

Impersonation using a computer resource, Cheating by means of impersonating a person using a computer resource or electronic device is punishable with imprisonment up to 3 years, and a fine up to INR 100,000.

Indian Penal Code**,** While there are specific offences detailed in the IT Act, a person can also take recourse under the general criminal law of India under certain provisions. There are various provisions of the IPC that may include cybercrimes as an offence:

Cheating[4]**,** the offence of cheating includes deceiving someone to deliver a property to a person, which he would not have delivered ordinarily if not deceived. In relation to a cyber offence, this could include deceiving someone to send across restricted or confidential data to a person not authorized to receive it, which the person so deceived would have ordinarily known and not sent.

Forgery of electronic records**,** This provision makes specific reference to an act with respect to any electronic document, making it a cybercrime. It includes making a false document or electronic record that would either cause damage to another person, or even leading to a false claim on a property. If done with the wrongful intention of committing such an act, it would be said to be forgery, punished with up to 2 years of imprisonment.

Similar to the IT Act offence, if a person intentionally receives or keeps a stolen property (say on electronic device) knowing it to be stolen may be punished up to 3 years of imprisonment. However, it is a settled position that a special law (in this case, the IT Act) prevails over a general law (i.e., IPC).13 Hence, if the offence committed is covered under the IT Act as well as the IPC, a charge for commission of such offence can only be made out under the IT Act.

[4] the Indian Penal Code, 1860

1.3.1. Procedure for Reporting and Prosecution of Cybercrime:

Depending on the nature of the offence (cognizable or non-cognizable), the police will either reduce the information in the form of a First Information report ("FIR")[5] 14 or refer the person to the magistrate after recording such information.15 After this, the police commences the investigation (or is directed to investigate by the magistrate16) relating to the offence, consequent to which, a criminal proceeding ensues when the magistrate feels there is sufficient reason to proceed

1.3.2. Register Complaint with National Cyber Crime Reporting Portal:

Cybercrimes can be reported only through the National Cyber Crime Reporting Portal.18 As mentioned above in Section 3(B)(i), this portal is an initiative of the Indian government to facilitate complainants/ victims to report cybercrime complaints online. It provides two options for reporting cybercrimes on the portal: (1) Report Crime related to Women/ Child or (2) Report Other Cybercrimes. Other cybercrimes would include the offences relating to cyber security such as online financial frauds, ransom ware, hacking, crypto currency crimes and online cyber trafficking as detailed in this section above. While all Indian citizens can report cybercrimes through this portal, the FAQs also state that a complaint can be filed by a person who is not an Indian citizen but has been victimized online by an individual or a company in India.19 Presently, over 30 cities in India have a cyber cell of their own, and the other towns and villages in the state have a separate dedicated cyber cell.

1.4. ROLE OF LAW ENFORCEMENT AND CYBERSECURITY PROFESSIONALS :

Law enforcement agencies and cyber security professionals play a vital role in combating cybercrime. The roles are given below-

- **Investigating Cybercrimes:** Law enforcement agencies have the proper cybercrime units, which investigate cybercrime and gather evidence against it. Sometimes they collaborate with forensic departments and cyber security branches to fight against cybercrime.
- **Response against Cybercrime:** The professionals are responsible for the recognizing, analyzing, and responding to cybercrime, like data breaches, malware attacks, and cyber-attacks, within organizations and government infrastructure.
- **Digital Forensics:** digital devices, computer systems, and network traffic are examined by the Forensic experts to analyze and extract evidence to support cybercrime investigations and prosecutions.
- **Cyber security Awareness:** Law enforcement and cyber security professionals play a crucial role in training and educating people, businesses, and organizations on best practices, and the prevention of cybercrime.

[5] Criminal Procedure Code, 1973

- **International Collaboration:** cybercrime is borderless in nature. So that there is a need for international cooperation and coordination among law enforcement agencies, cyber security agencies, and legal branches for the investigation and prosecution of cybercrime, across different jurisdictions.

1.5. Case studies under Cyber Law

The landmark case studies under cyber law aren given below-

i. ICICI Bank Phishing Case (2003):

In this case, hackers used a phishing attack to mimic ICICI Bank's website, tricking users into revealing their login credentials and personal information. It affected user's financial losses and damage to the bank's reputation.

The incident prompted legal action under the IT Act, focusing on offenses related to unauthorized access and data theft.

ii. Shreya Singhal vs. Union of India (2015)[6]:

This landmark case challenged Section 66A of the Information Technology Act, which was criticized for being overly broad and prone to misuse to curtail freedom of speech. The Supreme Court of India declared Section 66A unconstitutional, emphasizing the importance of safeguarding freedom of expression online.

iii. Indira Jaising vs. Supreme Court of India (2017):

These case highlighted issues related to the publication of judgments and sensitive case related information online. The court addressed the need for grater cyber security and confidentiality in the handling of legal documents and judgments.

iv. Ransomware Attack on Karnataka Power Corporation Limited (2020):

The Incident was a ransomware attack targeted at the systems of Karnataka Power Corporation Limited. Impact was disruption of power supply operations and financial losses.

Investigations ensued to identify the perpetrators and address the cybercrime, underscoring the risks associated with Ransomware attacks on critical infrastructure.

v. Data Breach at Air India (2021):

Air India faced a significant data breach, exposing sensitive personal information of millions of its passengers. They compromised passenger data, potential identity theft, and damage to the airline's reputation.

Investigations were launched under data protection provisions of the IT Act, emphasizing the importance of securing personal data.

vi. The Diginoter case is a landmark event in the realm of cyber law.

Diginoter, a Dutch certificate authority(CA) issued digital certificate crucial for securities online communication. In 2011, attackers compromised the diginoter system and issued fraudulent certificates, jeopardizing online trust and security.

[6] AIR 2015 SC 1523

In September 2011, after it had become clear that a security breach had resulted in the fraudulent issuing of certificates, the Dutch Government took over operational management of Diginoter's system. In the same month, the company declared it bankrupt.

vii. USA vs. Park Jin Hyok (North Korea case)

Park Jin Hyok was a North Korean hacker of the Lazarus group, which is a cyber criminal organisation under the Korean Government.

Park Jin Hyok committed the Sony pictures hack in 2014, Wanna Cry ransomeware attack in 2017 and extracted 81 million dollars from Bank of Bangladesh.

In September 2018 U.S imposed charges on Park Jin Hyok, on the grounds of computer fraud, digital abuse, identity theft, wire fraud.

viii. Vietnam Case of Cyber espionage

Vietnam cyber spies, alleged to be targeting Chinese government agencies to uncover the Covid-19 situation and valuable information.

The hackers working on the behalf of the Vietnam government to collect the Covid-19 pandemic response of China.(Published by Fire Eye)

ix. Petya Ransomware

Petya is a strain of ransomware that was first identified in the year of 2016. Like other types of ransomware, Petya encrypted files and data on the victim's computer. The operations of Petya demand payment in the Bit coins before they will decrypt the files and make them usable again. Unlike some older ransomware strains, which only encrypt certain important files in order to extort the victim. Petya locks up a computer's entire hard disc especially when it encrypt a computer's master file table, making it impossible to access any file on the hard disc. Petya has only been observed targeting computers with windows operating systems.

x. Not Petya case

Following are the three steps that can help if Petya or not Petya attack for less likely-

1. Strengthening email security practice.

Most Petya attacks and some Not Petya attacks, started with an infected email attachment. To prevent this, organizations can scan emails for malware, block email attachments from internal sources and train users to avoid opening untrusted attachments.

2. Regular Patching vulnerabilities.

The Eternal Blue exploit used by Not Petya had an available patch months before the attacks took place. Ransomware attacks in general often exploit software vulnerabilities to either enter a network or laterally within it. Updating software and Patching vulnerabilities can help eliminate these attacks vectors.

3. Backing up files and data. Organization can also adopt cloud flare one. It is a platform that helps users securely connect to the resources they need. Using a Zero Trust Security approach, Cloud flare one, helps to prevent and contain ransomware infection.

Conclusion

Now digital age ushered in a new era of criminal activities, collectively known as a cyber crime. Now computer technologies and the internet continuous to grow. This study has founded the intricate world of cyber crime. There are various types of cyber crime and highlighting the various challenges faced in combating these digital threats. From the jurisdiction issues and the anonymity of the internet to the rapidly evolving nature of technology and the need for international cooperation, the challenges are multifaceted and complex.

Cyber attacks can originate from anywhere in the world but jurisdiction over these crimes is often unclear. Hacker can stay one country and victim can stay another country. It is very difficult to determine which law apply and which authorities have the right to investigate and prosecute. Tracing cyber attacks back to their source id extremely challenging. Hackers can easily hide their identities and crime location, making it hard to determine who is responsible.

As the digital landscape expands, so does the threat of cyber crime. In India, the Information Technology Act, 2000, serves as the backbone of the legal framework for combating cyber crime and promoting cyber security. However, it is important to continuously update and strengthen cyber laws to keep pace with evolving cyber threats. Through a combination of robust legislation, technological advancements, and public awareness, India can build a safer digital environment for its citizens and effectively combat cyber crime. It is always advisable to consult Cyber Crime Lawyers if you are facing any problems related to cyber crime for a perfect legal solution.

REFERENCES

1. Cyber Laws by Dr. Gupta & Agarwal
2. Computers Internet and New Technology Laws 3rd Edition 2021 by Karnika Seth
3. Technology Laws Decoded by N S Nappinai
4. Law of Cybercrimes in India by K.M. Muralidharan & R. Singaravalan
5. Information Technology Law by Dr. S.R. Myneai
6. The Indian Cyber law by Suresh T. Viswanathan