ILE LEX SPECULUM

VOLUME I AND ISSUE I OF 2023

APIS – 3920 – 0036 | ISBN - 978-81-964391-3-2

Published by

Institute of Legal Education

https://iledu.in

CYBER CRIME – AN ANALYSIS

AUTHOR: JAISIKA BANSAL, STUDENT OF MAHARISHI MARKANDESHWAR (DEEMED TO BE UNIVERSITY)

BEST CITATION - JAISIKA BANSAL, CYBER CRIME – AN ANALYSIS, *ILE LEX SPECULUM (ILE LS),* 1 (1) OF 2023, PG. 185-191, APIS – 3920 – 0036 | ISBN - 978-81-964391-3-2.

Abstract

As we all know that this is the era where most of the things are done usually over the internet from online dealing to online transactions. Since the web is considered a worldwide stage, anyone can access the resources of the internet from anywhere. The internet technology has been used by a few people for criminal activities like unauthorised access to the other's network, etc. These criminal activities or offences/crimes related to the internet are cyber crimes. In this paper we focus on types of cyber crime and covers judgement in which the court held that it is an offence under various sections. We can define cyber law as a part of the legal system that deals with internet cyberspace and legal issues. Generally, it is alluded to as the law as the web. It covers a broad area encompassing many topics.

Keywords - Cyber crime, Digitalisation, Phishing, hacking, Identity theft, internet fraud

Introduction:

The internet is the global system of interconnected computer internet that uses the internet protocol suite to link billions of devices worldwide. Today, the internet is one of the most important parts of daily life. The information technology revolution has brought two main functions with the internet. On one hand it has contributed position values to the world. On the other hand, it has produced many problems that threaten the order of the society and also produce a new wave of crime in the world. The internet in India is growing rapidly. It has given rise to new opportunities in the field of entertainment, business, sports, education, and many more. With the advent and increasing use of the internet, businesses have crossed the barriers of local markets and are reaching out to customers located in every part of the world. With the advent of technology and digitalisation people have the ability to communicate virtually with anybody, anytime and anywhere across the globe. Cyber-crime has emerged as one of the results of modernisation. Cyber security is a technique developed to safeguard information and information systems which are stored on computers. The need for cyber security is due to the increase in cyber crimes or online crimes. Cybercrimes are committed using the internet and computer to steal the person's identity or illegal activities.

There are different names of e-crimes such as: high-tech Crimes, white collar crimes, and cybercrimes. Every year there is an increase of e-crimes due to the development of information technology and software changes. Thus e-crimes have become very common and spread via various methods including malicious programs, which are specially prepared to break through personal computers or enterprise systems for copying confidential information or destroying systems.

The abuse of the internet has given birth to new age crimes which are addressed by the Information Technology Act, 2000. As information around the globe has become more accessible, it has also become more vulnerable to misuse. India is on the radar of cyber criminals with growing cyber-attacks on the Indian establishment. India ranks third as a source of malicious activity on the internet, second source of malicious code and fourth and eight as source or original for web attacks and network attacks.

What is Cybercrime?

Cybercrimes is a criminal activity that involves a computer, networked device or a network. Most cyber crimes are committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. Cybercrime can be carried out by individuals or organisations. Some cybercriminals are organised, use advanced techniques and are highly technically skilled.

Cybercrimes can be defined as: "Offences that are committed against individual or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunications networks such as Internet (network including chat rooms, emails, notice boards and groups) and mobile phones".

Beginning and Growth of Cyber Crimes:

The history of cyber crimes is a complex and evolving one, with many different factors contributing to its growth over time. Here are some key points:

- The modern history of cybercrime began in the 20th century, when cybercriminals became early adopters of technology and used their head start to engineer new ways to part people and organisations from their data and money.
- The 1990s saw the rise of the internet and growth of cybercrime, as hackers and bad actors leveraged the fact that trust and safety controls weren't initially a major concern.
- Cybercrime has evolved alongside technology, with criminals seeking to exploit weaknesses in the system for personal gain or to prove a point.
- The first-known hacks occurred in the 1830s, when two thieves infiltrated the French telegraph system and stole data.
- The 1980s saw the rise of email and the first instances of Cybercrime involving viruses and scams.
- The 1986, hacking became a punishable crime under the Federal Computer Fraud and Abuse Act in the USA
- As technology has advanced, so have cybercriminals, with attackers becoming smarter and more innovative.
- Cybercrime has caused nearly $6 trillion in damages since the 1980s.
- Social networking has become an increasingly important tool for cybercriminals to recruit people to assist their money laundering operations around the globe.

Objective of Study of Cybercrime:

- To understand the types of crimes committed.
- To identify the individual and groups that engage in cybercrime.
- To develop measures to prevent and counter cybercrime.
- To raise awareness about cybercrime.

Impact of e-crimes:

E-crimes affect the community in many ways. This includes:

- Loss of online business and consumer confidence in the digital economy,
- The potential for critical infrastructure to be compromised affecting water supply, health services, national communication, energy distribution, financial services, and transport,
- Loss of personal financial resources and the subsequent emotional damage.
- Loss of business assets,

- Stimulating other criminal activity, or

- Costs in time and resources for law enforcement agencies.

Literature Review:

Knowing and being ready is the first line of protection against cyber threats and cybercrimes, e.g. by information security training. Training can take two forms; the first is aimed as security professionals and aims to improve understanding of the latest threats and to increase skills level in defending and mitigating against them. The aim of this paper is to research the idea of cyber range, and to include a comprehensive analysis of literature covering unclassified cyber ranges and safety test beds.

Aparna and Chauhan:

The authors in their paper conducted a research Tricity on cybercrime awareness and revealed that awareness can be increased by giving due importance to Cybercrime which can be an efficient tool to decrease or prevent the cybercrimes. They also concluded that it remains the responsibility of the net users as well as the government to ensure a safe, secure, and trustworthy computing environment.

Archana Chanvvai Narahari and Vrajesh Shah:

The author conducted a survey on 100 respondents to analyse whether netizens are really aware of cybercrimes. They found that the respondents are somewhat aware of the cybercrimes, cyber security but still there is a need to increase awareness among them. Also, they suggested a conceptual model explaining how to uphold and implement the awareness programs among internet users regarding cybercrimes.

Research Methodology:

The information throughout my study is collected through the secondary data.

Sources of secondary data: the information which is collected from the source which is earlier published in any of the forms known as secondary and second hand data. There are two types of sources: internal source and external source. The literature review of any research t is popularly known on secondary data mostly from books, articles and various research papers. The research methodology throughout my study is fully based on secondary data wherein all the information is collected by various sources and by referring various articles, research papers and books.

Research Questions:

- What are the legal consequences of committing cyber crimes?

- What are the measures taken to prevent and combat cybercrimes?

- How do cyber laws differ from traditional laws?

Observations:

What are the different types of Cybercrimes?

The different types of Cyber crimes can be classified into several categories. Here are the most common types:

- **Individual Cybercrimes:** These types of Cybercrimes target individuals and include activities such as phishing, spoofing, spam, cyberstalking, and identity theft.

- **Organisational Cybercrimes:** This category focuses on targeting organisations. It involves crimes committed by teams of criminals, including malware attacks and denial-of-service attacks.

- **Property Cybercrimes:** This type of cybercrime targets property, such as credit cards or intellectual property rights.

- **Social Cybercrimes:** This is the most dangerous form of Cybercrime, as it includes cyberterrorism. It involves acts that threaten the safety and security of society as a whole.

Some common example of Cybercrimes within these categories include:

- **Phishing and Scams:** This refers to the act of tricking individuals into revealing sensitive information, such as passwords or credit card details, through fraudulent emails or websites.

- **Identify Theft:** This involves stealing someone's personal information, such as their social security number or bank account details, to commit fraud or other illegal activities.

- **Ransomware Attacks:** This type of Cybercrime involves encrypting a victim's data and demanding a ransom in exchange for its release.

- **Hacking/ Misusing Computer Networks:** This refers to unauthorised access to private computers or networks and the misuse of them, such as shutting them down or tampering with them.

- **Internet Fraud:** This includes various fraudulent activities conducted online, such as online scams, pyramid schemes, or fake online marketplace.

Social media, cybercrimes and cyber laws:

Social media has become a platform for cybercrimes, and cyber laws have been out in place to deal with these crimes. Cyber laws are specific legislations that penalise cybercriminals and attempt to reduce crimes in the technological domain. Cybercrime refers to wrongful acts that are conducted over a computer or through networks using digital technology.

Cybercrime is social media that includes circulation and distribution of illegal, prohibited, or explicit content that can be offensive, disturbing, or wrongly influential.

There are different types of Cybercrimes, including crimes against people, property, and the government. Although Cybercrimes are a global issue, the laws for cyber crimes differ from country to country. Cyber law is increasing in importance every year because cybercrime is increasing. Recent trends in cyber law include new or more stringent regulations, reinforcing current laws, increased awareness of privacy issues, cloud computing, how virtual currency might be vulnerable to crime, and usage of data analysis.

Cyber Laws in India:

Cyber law in India is governed by two key legislations: the Indian Penal Code and the Information Technology Act of 2000. The Indian Penal Code covers traditional criminal activities such as theft, fraud, forgery, defamation, and mischief, all of which are subject to the Indian Penal Code. The Information Technology Act, 2000 addressed new age crimes that are committed using computers and the internet. Cyber law in India encompasses a broad range of subjects, including intellectual property rights, privacy rights, and cybercrime.

The following are some of the key aspects of cyber law in India:

- Cybercrime is any crime committed using technology and a computer as a tool.

- Citizens are prevented from sharing private information with strangers online by cybercrime laws.

- Cyber law in India protects online users from harassment and stalking.

- The theft of identities, credit cards, and other finance- based crimes are addressed by Indian cyber laws.

- Cyber law in India provides recognition to electronic documents and a framework to support e-filing and e-commerce transactions.

India's cyber laws have helped to enable electronic commerce and electronic governance to flourish in India by safeguarding maximum connectivity and minimising security concerns. They allow individuals or organisations to take legal action against someone if that person violates and breaks the provisions of the law.

Landmark Judgement:

- **CBI v. Arif Azim (Sony Sambandh Case)**

A website called www.sony-sambandh.com enabled NRIs to send Sony products to their Indian friends and relatives after online payment for the same. In May 2002, someone logged into the website under the name of Barbara Campa and ordered a Sony Colour TV set along with a cordless telephone for one Arif Azim in Noida. She paid through her credit card and the said order was delivered to Arif Azim. However, the credit card agency informed the company that it was an unauthorised payment as the real owner denied any such purchase.

A complaint was therefore lodged with CBI and further, a case under sections 418, 419, and 420 of the Indian Penal Code, 1860 was registered. The inventions concluded that Arif Azim while working at a cell centre in Noida, got access to the credit card details of Barbara Campa which he misused.

The Court convinced Arif Azim but being a young boy and a first time convict, the court's approach was lenient towards him. The Court released the convicted person on probation for 1st year. This was one among the landmark cases of cyber law because it displayed that the Indian Penal Code, 1860 can be an effective legislation to rely on when the IT Act is not exhaustive.

Legal Consequences:

Cybercrime is a serious offence that can result in significant legal consequences. The penalties for committing Cyber Crimes vary depending on the nature of the crime, the extent of any damage done, and whether the offender has previous offences. Here are some of the legal consequences of committing Cybercrime:

- **Fines:** Cybercriminals may be required to pay fines as a penalty for their crimes. The amount of the fine will depend on the nature of the crime and the extent of the damage caused.

- **Imprisonment:** Cybercriminals may face improvement as a penalty for their crimes. The length of the sentence will depend on the nature of the crime and the extent of the damage caused. For example, some cybercrimes may result in a sentence of up to 20 years in prison.

- **Restitution:** Cybercriminals may be required to pay restitution to their victims as a penalty for their crimes. This may involve compensating victims for any financial losses or damages they suffered as a result of the Cybercrime.

- **Probation:** Cybercriminals may be placed on probation as a penalty for their crimes. This may involve restrictions on their activities, such as a ban on using the internet or computers.

- **Loss of privileges:** Cybercriminals may lose certain privileges as a penalty for their crimes. For example, they may lose their right to vote or own a firearm.

Measure to Prevent:

- **Awareness and education:** Spreading awareness about cyber crimes and educating individuals, organisations, and the general public about the risks and preventive measures is crucial. This can be done through campaigns, workshops, and educational materials.

- **Strong password and software updates:** Using strong, unique passwords and regularly updating software and applications can help protect against Cybercrimes.

- **Secure internet security suite:** Utilising a full-service internet security suite can provide comprehensive protection against various cyber threats.

- **Managing social media settings:** Being cautious about the information shared in social media platforms and managing privacy settings can help prevent Cybercrimes.

- **Strengthening network security:** Implementation Of robust network security measures, such as firewalls, intrusion detection system, and encryption, can help protect against cyber intrusion.

- **Collaboration and Cooperation:** Enhancing collaboration and cooperation among various stakeholders, including government agencies, law enforcement, private sector organisations and international partners, is essential in combating cybercrimes.

- **Investigation and prosecution:** Law enforcement agencies play a crucial role in investigating cybercrimes, apprehending perpetrators, and prosecuting them. This includes specialised cyber crime units and task forces.

- **Enhancing cybersecurity:** Strengthening cybersecurity measures at both individual and organisational levels is vital in preventing and combating cybercrimes. This includes implementing multi-factor authentication, data encryption, and regular security audits.

- **International Cooperation:** Cybercrimes often have a global reach, so international cooperation and information sharing are crucial in combating cyber threats. This includes sharing intelligence, coordination investigations, and extraditing cybercriminals.

- **Holistic approach:** Taking a holistic approach to the prevention, detection, and investigation of cybercrimes is essential. This includes using advanced technology, establishing cybercrime centres, and leveraging expertise from various fields.

Suggestions:

- While using an online platform, not divulging any personal data is almost impossible and thus, one should beware while sharing any personal information online.

- It is imperative that an eye should be kept in phoney email messages and such emails should not be responded to that ask for personal information. Also, email addresses should be guarded.

- While engaging in online activities it is imperative that attention should be paid to privacy policies on websites and steer clear of fraudulent websites used to steal personal information.

- It is necessary that response to offences on the internet against women should be seen as part of the broader movement against harassment and abuse. Broader efforts should be initiated as it is ultimately a people- centred challenge.

- A collaborative effort among media, clubs, associations and women's media networks is critical to promote women's leadership and decision making in the society.

- Education systems must initiate contemporary issues regarding online crimes and awareness should be spread regarding safe internet users.

- The Government should make more rigid rules to apply on the Internet Service Providers (ISPs) as they have the entire record of the day that is accused by the users surfing on the web.

- Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our nation's cybersecurity objectives by investigating a wide range of cyber crimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible.

- Governments can build up capabilities, most of all law enforcement, to shore up gaps, particularly in developing countries. They can also strengthen international cooperation and collaboration to combat cybercrime.

- Governments can work to improve cyber law by adopting new and more stringent regulations, reinforcing current laws, increasing awareness of privacy issues, and addressing emerging technologies such as cloud computing and virtual currency.

Conclusion:

All the way through my research on Cybercrime and security will be helpful to spread the awareness among normal people about emerging security threats.

Cybercrime as a whole refers to 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 the internet and mobile phones. Such crimes may threaten a nation's security and financial health. Issues surrounding this type of crime 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 is the need of the hour to evolve the societal and cultural norms with the development of information technology. Technology has become an integral part of our daily life in the world of the internet and cannot be dispensed with. Although there are several advantages of the technology, it has become a threat to our lives too. Mandatory step that needs to be taken. Steps like digital literacy, development of data security, providing access to technology to individuals and groups of individuals and most of all enactment of laws specifically on Cybercrime.

" The law is not the be-all and end-all solution."

Reference:

- www.blogipleader.com
- www.livelaw.com
- www.drishtiias.com
- www.outlookindia.com