IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Law And Cyber Crime – A Comprehensive Study

Name of 1st Author Avneet kaur dhillon , Name of 2nd Author Reeta kumari

Designation of 1st Author Assistant Professor, Designation of 2nd Author Student

UNIVERSITY SCHOOL OF LAW

RAYAT BAHRA UNIVERSITY, KHARAR, INDIA

ABSTRACT:

"Cybersecurity is no longer just an IT issue, it is the responsibility of each individual to ensure trust in this digital world." Nappo Stephane Rules and regulations pertaining to computer technology, the Internet, and digital communications are provided by cyber law. incorporated. Computer networks, the Internet, and computers are involved in many aspects of cybercrime, including data protection, cybersecurity, cybercrime, intellectual property rights, and online commerce. Cybercrime by digital methods includes data theft, fraud, online harassment, hacking, and the dissemination of malicious software. Flash drives, microchips, DVDs, pen travel, and more are used by criminals. The primary issue is that the crime has a horrible appearance, particularly when it comes to child pornography and copyright violation. Numerous forms of cybercrime are covered in this study, such as virus assaults, cyberfraud, cyberterrorism, online annoyance, hacking, fishing, and cyberstalking. It also draws attention to the difficulties associated with cybercrime, including its jurisdiction, rapid technology advancements, documentation, and prevention. It also takes into account the legal and regulatory actions taken against cybercrime by states and international organizations. This covers worldwide corporate frameworks, national data protection strategies and regulations, cybersecurity, and cybercriminal law.

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

1.INTRODUCTION

"It's part of everyday life because technological advancements are based on the fact that it doesn't fit and pre vents it from happening. From education, entertainment, etc., this technology has a lot to do with it. There is . It is convenient and it has also become a criminal offence called cybercrime.

Cybercrime can take a variety of forms, including data theft, fraud, malware attacks, and phishing that interferes or damages your computer. The infinite feature of the Internet or cyberspace is that cybercrime has global issues with national restrictions, and challenges for law enforcement and legal professionals. Governments and international organizations have developed many legal and regulatory measures to control cybercrime, cybersecurity strategies, cyber law, data protection and data protection regulations. Criminal prosecutors play a key role in cybercrime investigations and carry out digital forensic advertising actions, including cybersecurity awareness. This comprehensive study should be conducted in cyber law and cybercrime research. and regulatory measures.

1.1.DEFINING CYBER LAW:

The Internet and Cyberspace Act is called cyber law, which includes legal questions and regulations Cyber laws regulate the use of computer technology, the Internet and communications.
Cyber Law covers the areas of intellectual property, data protection, data protection, online trading, electronic conferencing, cybersecurity and cybercrime prevention. Cyber law provides a legal framework for crimes. This is a challenge that arises in the digital age. The purpose of cyber rights is to protect individuals, businesses and society from cyber attacks and cyber threads, allowing for the responsible use of technology.

The function of cyber law:

- Data Protection and ProtectionAct provides protection measures for personal data or information.
- fields such as e-commerce, electronic contracts, and online financial transactions.
- After Cyber Law, intellectual property protects laws such as software, music, video and more.
- Illegal Online - Screams, Cybertrakes, frauds and screaming to protect their people.

AN DEFINITION OF CYBERCRIME

Cybercrime is a type of crime that requires computers and network participation. As tools, computer systems and networks can use crimes such as hacking malware attacks, phishing ,cyberstalking, online fraud, and cyberterrorism. Cybercriminals use computer technology to

obtain personal or sensitive data for malicious purposes. Use computers for communication and data storage. Criminals use cybercrimes to suffer massive amounts of data, money, or damage. At some point, it becomes greater than cyberterrorism. This is extremely dangerous for society and communities. Cybercrime The nature of cybercrime is a complex and evolving concept. His nature, as a whole, can reduce nature due to the border. Cybercrime activities are carried out using computers or computer networks and digital technologies. The nature of cyberbreak can be divided into several points.

- The nature of cybercrime is intangible.
- It is entirely dependent on technology and e-platforms, primarily virtual concepts.
- Its nature is borderless since it lacks geographical bounds.

- As technology develops, cybercriminals are constantly presented with new options, quick
- Another aspect of cybercrime is development.

Different kinds of cybercrime:

Crimes can be broadly classified under the phrase "cybercrimes," which encompasses a wide range of criminal activity. They're -

- **Hacking**:
  Hacking is similar to gaining illegal access to a network or computer system in order to steal information
  or cause damage. Simply put, this means illegal penetration into a computer system or network. The re is a concept of hacking known as cracking, but there is no difference between hacking and cracki ng from Indian legal scenarios. All actions split against a computer or network system called hackin g. Hackers primarily use computer programs to attack target computers. Some hackers chop for prof it by stealing credit card information or transferring money from the victim's bank account from the ir own.
- **Data Theft**:
  Data theft is a type of crime in which a criminal steals personal or valuable data by accessing compu ters, mobile phones, digital cameras, emails, websites, etc. Today, cybercriminals use data dates to t hreaten threats or earn money. This type of
  crime is easy for office workers with access to technology such as desktop computers,to store digital information such as flash drives, iPods, digital cameras, and even mobile phones. In other words, so meone without the owner's permission to monitor,
  download, download, copy, or extract data or other information from theft of such Computeris data.
- **Social Engineering and Phishing:**
  It's a technique that criminals don't like sharing information, they share them and manipulate them t o do what they should do. Phishing is a cybercrime technique in social engineering. Phishing is the act of attempting to steal usernames, passwords credit card data and other information from trustwor thy companies in electronic communications.Phishing is made from E
  Mailspoofing, and often leads users to enter their details on fake websites that look roughly the sam e as the original.
- **Cyberstalking:**
  This is a type of stalking carried out by digital technology to use data and information to harass and intimidate individuals. Stalking is a kind of annoying or threatening behavior that repeatedly involv es an individual. This can be done by telephone, written message, or by vandel of a person's propert y. Cybertalk can also be defined as repeated harassment files or as cybercriminal threatening behavio r against victims.

- **Email Spoofing:**

  This is a very common technique used in cybercrime. It's an email based scam. When a cybercriminal sends the victim to the victim as another person,company, or another bank or bank to obtain information. The purpose of e-mail-poofing is to provide confidential information credit card data, bank details, or click on malicious links that affect the system.

- **Malware attack:**

  This is a type of virus or software distributed by cybercriminals to damage, win or get in the way of computer systems. Creating and distributing malware in all countries is a serious crime, but it continues to be manufactured for a variety of reasons, including Showing your ability and earning money. Malware includes computer viruses, ransoms, worms, trojans, rootkits, spyware, adware, malignant BHOs, rogue security software, and other malicious programs that are extremely dangerous to information technology.

- **Child Pornography:**

  Child porn is a type of porn involving the content of a child or child. Porn uses a variety of media platforms, including magazines, photos, sculptures, paintings, cartoons, paintings, animations, sound recordings, movies, videos, and video games. Child porn can be simulated child porn or produced with the inperson participation of the child. Legal definitions of child porn generally include preliminary match, minors after shear cover or juve, sexual images containing computer-generated AI generated images that are likely to be involved. Includes: Most owners of child porn are arrested for having pictures of child role models.

- **Cyber Terrorism:**

  This is another type of crime caused by using digital technologies such as computers, networks, and the Internet to create obstacles, fear, and confusion in public or political goals. This includes the committee's cyber systems and infrastructure that affect critical services, national security, and the panic of the people. Cyberterrorists are individual or organized groups that aim to be infrastructure such as financial systems and government agencies.

1.2.2.Challenges in the fight against cybercrime

There are many laws relating to cybercrime, but changes should change in laws and regulations as cybercrime changes or changes over time and technology. . Fighting cybercrime has many challenges. This is explained below.

The Internet can be anywhere, so it can be national and international or global. This is a major challenge to identify crime liability. Laws and regulations must be adapted at a time to control the challenge. Evidence collided or preserved by digital means can be easily altered, damaged or destroyed. The collection and storage of computer systems is forensic and takes important measures in court.

- **Lack of expertise**: To combat cybercrime, experts specializing in cybersecurity, digital forensics an d skills are very minimal experts. Training and recruitment experts are the biggest challenge of this period.
- **Public perception**: Many cybercrimes have successfully used human weaknesses through hacking, phishing and social engineering. Sensitization of the public to cyber threats and promoting better cyb er practices can reduce crime.

1.1. India's Regulatory Framework

The National Cybersecurity Policy was dated 2013 and was established with the vision of building s afe and resistant cyberspace for citizens, businesses and governments. Risks to human life, economi c and national security. The guidelines also determined key strategies for protecting cyberspace. Mo st of them are applicable today. Politics took into account the fact that revised national policies for cybersecurity have been significantly postponed 10 years ago. In December 2022, the government e xplained that it had drafted a cybersecurity strategy for national cyberspace security. 2The details of the strategy and implementation schedule are not mentioned.

Information Technology Act, 2000 (IT Act) The IT Act provides punishment for, among other thing s, crimes related to electronic communications or data, and other crimes related to cybersecurity. Ce rtain crimes such as access to computers, computer systems, computer networks without the permiss ion of the responsible person from

the computer will download or copy data from the computer, and also allow the perpetrator to pay c ompensation for denying access to the computer. Masu. Crime, Section 43 of the IT Act is paid for certain actions related to computer infrastructure (i.e. computers, computer systems, computer netwo rks) and computer resources in the absence of owners or such computer persons. Compensation is sti pulated. Infrastructure or resource. This includes unauthorized access, downloading, introducing co mputer pollution, damage, and denial of access.

According to Section 66, these measures will be punished with a fine of up to 500,000 inches if dete ntion for up to three years and/or fraudulently or fraudulently carried out. If a person grants access t o material containing personal information about another person and knows that without the consent of the intended person, or that they are likely to be incorrect loss or illegal interests; Punishment wi ll be imprisoned and punished for up to 3 years and/or fines for up to 500,000 INR documents of co mputer sources, intentional veiling, destroying or modifying computer source code up to 3 years,an d/or fines for up to 200,000 INR . Fines up to 3 years and/or up to 100,000 INR. He is punished wit h a maximum of three years in prison and a fine of up to 500,000 INR.Imitation with computer reso urces that are cheating on people with computer resources or electronic devices will be punished wi th a maximum of three years in prison and a fine of up to 100,000 INR.Indian criminal law and IT la w have certain crimes, but people can also rely on them in accordance with certain provisions based on general criminal law.

There are.various IPC regulations that can include cybercrimes as Fraud. When it comes to cybercrimes, this can help someone to deceive someone to send limited or sensitive data to someone who has no right to acquire them.

Tamming of electronic records, this provision specifically refers to laws related to electronic documents that are cybercriminals. This includes electronic protocols that damage false documents or other people or undermine false claims against property. If carried out with the illegal intent to commit such an action, it would be said as a fake punishable by imprisonment for up to two years. Just like IT Code criminal offences, those who intentionally receive stolen property or stolen property (such as electronic devices) can know that they can be stolen in prison for up to three years. However, special laws relating to general laws (i.e. IPC) in this case IT law are defined as winning. Indictments for such crimes can only be issued under the IT Act.

1.3.1.Cyber Crime Cyber Reporting and Persecution Procedures

Depending on the type of crime (recognizable or unusable), the police will either reduce the information in the form of an initial information report (FIR) 14 or subsequently I'll introduce you to someone. Recording such information to the judge is reason enough to continue.

1.3.2.Register complaints regarding cybercrime reporting:

Cybercrimes can only be reported via the National Cybercrime Reporting Portal/Victim to report cybercrime criminal charges online. It offers two options for reporting cybercrime on the portal.

(1) Report a crime related to reporting a woman/child or

(2) other cybercrime. Other cybercrimes include crimes related to cybersecurity, such as online finance fraud, ransom boxes, hacking, cryptocurrency breaks, and online cyber trade, as explained in this section above. All Indian citizens can report cybercrimes about this portal, but the FAQ also indicates that complaints have been made by people who are not Indian citizens but have been victimized online by Indian people or companies. indicates. India, its own cybercells, and other cities and villages in the state, have their own dedicated cybercells.

1.4.The role of law enforcement and cybersecurity experts:

Law enforcement and cybersecurity experts play an important role in the fight against cybercrime. The role will be carried over to the bottom. Sometimes they work with the forensic department and cybersecurity branches to combat cybercrime.

Response to Cybercrime: Experts are responsible for their perception, analysis and respons to cybercrime, such as data damage, malware, cyberattacks within an organization and state infrastructure.

Digital Forensics: Digital devices, computer systems and network traffic are investigated by forensic experts to analyze and extract evidence of cybercrime investigation and persecution support.

Cybersecurity Awareness: Law enforcement and cybersecurity experts play an important role in training a nd training people, businesses and organizations, and preventing cybercrime for best practices. It's essential ly rimless. Therefore, there is international cooperation and coordination between law enforcement, cyberse curity authorities and the right branches for the investigation and persecution of cybercrimes in various juris dictions.

1.5.Cyber Law Case Study

The pioneering case studies using Cyber Law are shown below.

i.ICICI Bank Phishing Case (2003):

Users will reveal their login information and personal information. It affected the financial losses of users a nd the damages of bank calls. The case took legal action in the context of IT law and focused on crimes rela ted to unauthorized access and data theft.

ii. Shrðµya Singhal vs. Union of India (2015):

This groundbreaking incident called for Section 66A of the Information Technology Act. The Supreme Cou rt of India declared Section 66A unconstitutional and emphasized the importance of securing frðµthe online from ðmµssion.

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

In this case, questions relating to judgment and publication of sensitive cases were highlighted online. The court spoke about nðgradgrad's cybersecurity and confidentiality in the handling of legal documents and de cisions.

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

This incident was a ransomware Attack on Karnataka Power Corporation Limited's system. The effects wer e obstacles to power trading and financial losses. Research is working to identify perpetrators and improve cybercrime, creating risks associated with ransomware attacks in critical infrastructure.

v. Data Injury to Air India (2021):

Air India has been stopped before a serious data injury and has set up sensitive personal in formation from millions of passengers. They impaired passenger data, potential identity theft and damage to airline calls. Research has begun as part of the IT Act's data protection regulations, which underscores the i mportance of securing personal data.

vi. The Diginoter case is a pioneering event in the cyber rights field.

In 2011, attackers put the Diginoter system at risk and issued fraud certificates. In September 2011, the Dut ch government took over in September 2011. I realized that a security violation led to an unauthorized displ ay of the certificate. In the same month, the company explained it had gone bankrupt.

vii. America vs. Park Jin Hee-ok (North Korea Incident) Park Jin Hee-

ok was a North Korean hacker of the Lazaro Group, a cybercriminal organization under the South Korean g overnment. Park Jin Hyok committed to Sony Pictures Hack in 2014. Ransomeware2017 wants to extract $ 81 million from the Bank of Bangladesh, calling for the Ransomeware attack. In September 2018, USA Pa rk Jin Hyok charged computer fraud, digital abuse, identity theft and wire fraud.

viii. Vietnamese cyberspy.

Hackers working on behalf of the Vietnamese government will collect Covid 19 pandemic responses in Ch ina. Since 2016. Like other types of ransomware, it encrypts Petia files and data on the victim's computer.

ix.Petya Ransomware

Petya operations require payment in Bitcoin before deciphering the file and making it available for use agai n. In contrast to some older ransomware trunks, they encrypt only certain important files to blackmail victi ms. Petya blocks the entire computer's hard CD,
especially encrypting the computer's master files, preventing you from accessing the files on the hard CD. It was only observed that Petya uses the Windows operating system to target computers. Enhanced email sec urity practices.

x.Not Petya case

Most attacks by Petia and some Petia attacks began with infected E-mile attachments.

1.To prevent this, companies can scan emails with malware, block e-
attachments from internal sources, and train users to not open trusted attachments.
2. Regular patching of weak spots. The eternal blue exploit used by not Petia had a patch available a few mo nths before the attack. Ransomware attacks generally use software weaknesses to enter the network or side. Update your software and patch your weaknesses to help you remove these attacks.
3. File and data security. Organizations can also use cloud flares. This is a platform that helps users connect securely to the resources they need. With Zero-Trust
Security approach, Cloudflare 1 helps prevent and contain ransomware infections.

CONCLUSION

Today, the digital age is emerging in a new era of criminal acts, collectively known as cybercrime. Currently, I grow computer technology and the internet. This study founded a complex world of cybercrime. There are different types of cybercrime, highlighting the various challenges in combating these digital threats. From the issues of responsibility and

the anonymity of the Internet to the rapidly developing nature of technology and the need for international cooperation, the challenges are multifaceted and complex. not clear. Hackers can remain a country, and victims can remain another country. It is extremely difficult to determine which laws and which authorities have the right to consider and pursue a crime. Tracking cyberattacks with SourceID is extremely difficult. Hackers can easily hide their identity and location of crime. This makes it difficult to determine who is responsible. There is also the risk of cybercrime in digital landscapes. In India, the Information Technology Act of 2000 serves as the backbone of the legal framework to combat cybercrime and promote cybersecurity. However, it is important to continuously update and strengthen cyber laws to keep up with the development of cyber threats. A combination of robust law, technological advancements and public awareness allows India to effectively fight a safer digital environment for its citizens and effectively fight cybercrime. If you have problems related to cybercrime for a complete legal solution, we recommend consulting with an attorney about cybercrime.

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