INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER CRIME AND CYBER LAW: A COMPREHENSIVE ANALYSIS

AUTHORS - KRISHAN CHAND* & MS. NAVDEEP KAUR**, LLM SCHOLAR* & ASSISTANT PROFFESOR** AT LLM AT SANT BABA BHAG SINGH UNIVERSITY, JALANDHAR

BEST CITATION - KRISHAN CHAND & MS. NAVDEEP KAUR, CYBER CRIME AND CYBER LAW: A COMPREHENSIVE ANALYSIS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (1) OF 2025, PG. 1107-1114, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT:

"Cyber security is no longer just an IT issue, but the responsibility of every individual to ensure trust in this digital world." Nappo Stephane Regulations pertaining to computer technology, the internet, and digital communications are all included in cyber law. It covers a wide range of topics, including online transactions, cyber security, cybercrime, intellectual property rights, data privacy, and data protection. Cybercrime, on the other hand, describes unlawful actions involving computers, computer networks, and the internet. Cybercrime includes data theft, fraud, online harassment, hacking, and the dissemination of malicious software. This is carried out via digital channels. DVDs, pen drives, flash drives, microchips, and other devices are used by the thief. The primary problem is that the crime takes a terrible form, especially when it comes to copyright violations, child pornography, etc. Hacking, fishing, cyberstalking, online harassment, virus assaults, cyberfraud, cyberterrorism, and other forms of cybercrime are all included in the study. The difficulties of cybercrime, its jurisdictions, the speed at which technology is developing, the gathering and prevention of evidence, etc., are also highlighted by this. It also examines the laws and rules pertaining to cybercrime that have been put in place by the government and international organizations. This covers international corporate frameworks, data protection and privacy legislation, cybercrime laws, and national cyber security policies.

Keywords: technology, hacking, data theft, cybercrime, privacy, and protection.

INTRODUCTION

"Technological advancements are based on integrating into daily life so that you don't really notice them." Bill Gates Education, communication, entertainment, and other aspects of human life have been altered by technology and the internet in this digital age. It is now easier than ever to use the internet, technology, and human living. Due to technology and electronic means, the entire world is now connected to a vast amount of data and information that is continually changing. Although new technology has made many things more convenient and easy, it has also resulted in a crime known as cybercrime. The exchange of vast amounts of data online makes data breaches and privacy violations a component of cybercrime. The primary objective of the cybercriminals waspersons or businesses to profit while hurting others. Legal frameworks and tactics to address cyber dangers are necessary as technology and digital systems advance. Cybercrime, which aims to interfere with or harm computers, can take many different forms, including phishing, virus assaults, fraud, and data theft. Due to the internet's or cyberspace's lack of national borders, cybercrime is a worldwide problem that presents difficulties for law enforcement and legal experts. The speed at which technology is developing makes it extremely challenging to choose the appropriate jurisdiction. To combat cybercrime, the government and international organizations created a number of legal and regulatory measures, including data protection and

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

privacy legislation, cyber security plans, and cyber laws. Law enforcement organizations are essential to the investigation process. cybercrimes, carrying out digital forensics, raising awareness of cyber security, etc. The goal of this thorough study is to offer an in-depth examination of cybercrime and cyberlaw, including the many legal and regulatory measures as well as the kinds of difficulties that arise.

WHAT CYBER LAW IS :

Cyber law encompasses the legal issues and legislation pertaining to the internet and cyberspace. Cyber law regulates communication, the internet, and computer technology use. Intellectual property rights, data privacy, data protection, online transactions, e-contacts, cyber security, and cybercrime prevention are all covered under cyber law. A legal framework for crime and other issues that come up in the digital age is provided by cyber law. Cyber law's goal is to shield people, companies, and society from online threats and to empower the accountable use of technology.

CYBER LAW'S ROLE:

- Laws pertaining to data privacy and protection offer protection for private information.
- Cyber law makes ensuring that data management procedures are used correctly.
- Online financial transactions, e-contracts, and e-commerce are all governed by cyber law.
- Software, music, films, and other digital content are protected by intellectual property rights under cyber law.
- Cyber laws assist in identifying unlawful online behaviors such as fraud, cyberstalking, and hacking and offerprotections from this for people.

CYBERCRIME DEFINITION

Cybercrime is a category of criminal activity that requires the use of a computer and a network. Computer systems and networks can be used as a weapon for crimes such as child pornography, online fraud, cyberterrorism, phishing, hacking, virus attacks, and cyberstalking. Cybercriminals exploit computer technology to obtain sensitive or confidential information for their own nefarious ends. They communicate and save data on computers. Cybercrime is used by criminals to get vast quantities of data, money, or to do harm to others. Sometimes it becomes more serious, like cyberterrorism, which poses a serious threat to the community or society. The characteristics of cybercrime Because it has no boundaries, cybercrime is a vast notion that is constantly changing. Computers , computer networks and digital technologies are used to carry out cybercrime activities. A few categories can be used to categorize the nature of cybercrime:

- The nature of cybercrime is intangible.
- It is entirely dependent on technology and e-platforms, primarily virtual concepts.
- it has no territorial limits, making it borderless; and as technology advances, cybercriminals are constantly presented with new chances.
- Another aspect of cybercrime is development.

TYPES OF CYBERCRIME:

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

- **Hacking:** hacking is like illegal access to the computer system or network to steal data or information or cause damage. Simply simply, it refers to an unauthorized entry into a network or computer system. Although hacking is sometimes referred to as cracking, there is no distinction between the two in Indian legal terminology. Hacking is any action used to gain access to a computer or network system. Computer programs are the primary tool used by hackers to target computers. By

transferring funds from victims' bank accounts to their own or collecting credit card information, some hackers hack for financial gain.

- **Data Theft:** A sort of crime known as "data theft" occurs when a thief gains access to a person's computer, cell phone, digital camera, email, website, and other devices in order to steal their valuable or personal information. Cybercriminals now utilize the process of data theft to threaten or profit. Office workers who have access to devices like desktop computers that can store digital data, such as flash drives, iPods, digital cameras, and even mobile phones, find it easy to commit this type of crime. Put another way, it is considered data theft if someone who manages a computer or computer system downloads, copies, or extracts any data or information from it without the owner's consent.
- **Social Engineering and Phishing:** Criminals use this tactic to coerce people into doing things they shouldn't, like revealing information, but they do. Phishing is a type of cybercrime that involves social engineering. Phishing is an act of attempting to steal information such as usernames, passwords and credit card numbers by a trustworthy person via electronic contact. Phishing is a type of email spoofing that frequently leads consumers to enter personal information on a phony website that nearly appears the real one.
- **Cyberstalking:** This type of stalking uses digital technologies to threaten or harass someone by leveraging their information or data. A person who persistently engages in unpleasant or threatening behavior is said to be stalking. It can be accomplished by making phone calls, sending written messages, or damaging someone else's property. Another way to describe cyberstalking is when a cybercriminal repeatedly uses internet services to harass or threaten the victim.
- **Email Spoofing:** This strategy is frequently employed in cybercrime.It is somewhat of an email scam. when cybercriminals send victims emails pretending to be someone else, a business, or a bank in order to obtain their personal information.The goal of email spoofing is to trick recipients into divulging private information, such as bank account information or credit card numbers, or into clicking on links that could compromise their systems.
- **Malware attack:** Cybercriminals use this type of program or virus to harm, obtain information, or interfere with computer systems.Although creating and disseminating malware is illegal in every country, it is nonetheless done for a variety of reasons, including showcasing one's skills or generating revenue. Computer viruses, ransomware, Trojan horses, worms, root kits, spyware, adware, malicious BHOs, rogue security software, and other harmful applications are all considered malware, and they pose a serious threat to information technology.
- **Child Pornography:** A type of pornography that features children or kid-related information is known as child pornography. A variety of media platforms, such as magazines, photographs, sculptures, drawings, cartoons, paintings, animation, sound recording, film, video, and video games, are used in pornography. A child may directly participate in the production of child pornography or it may be mimicked. Sexual photographs of prepubescent, pubescent, or postpubescent minors as well as computer-generated or artificial intelligence (AI)-generated images that seem to feature them are typically included in legal definitions of child

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

pornography. Because they have pictures of youngsters who are not yet adolescent, the majority of people who possess child pornography are caught..

- **Cyber Terrorism:** This kind of crime involves the use of digital tools, like computers, networks, and the internet, to disrupt, frighten, and destabilize public or political goals. It entails taking advantage of cyber systems and infrastructure to launch attacks that jeopardize national security, vital services, and public confidence. Cyber terrorists can be individuals or organized groups, target the infrastructure like financial systems and government agencies.

TROUBLES IN THE FIGHT AGAINST CYBERCRIME

Even if there are numerous laws that address cybercrimes, rules and regulations need be updated because cybercrime evolves with time and technological advancements. Fighting cybercrime has a number of difficulties. They are talked about below:

- **Jurisdictional Issues**: Cybercrime is defined as any crime committed in cyberspace that has no restrictions or borders. Due to the widespread usage of the internet, it can be both national and international or global in scope. so that determining the jurisdiction of the offense becomes extremely difficult.
- **Rapid Technological Evolution**: With the development of new technologies, technology is constantly changing.To conceal and safeguard their operations, the thieves make use of cutting-edge technology. To control the challenges, laws and regulations must change throughout time.
- **Evidence Collection and storing:** For the crime to be identified, digital proof is crucial. Digitally collected or stored evidence is susceptible to modification, corruption, and destruction. It takes a great deal of skill to gather and preserve evidence from computer systems that is forensically admissible in court.
- **Shortage of Expertise**: Professionals with expertise in digital forensics and cybersecurity who are equipped to tackle complex cybercrimes are extremely rare. The largest problem in this day and age is hiring and training professionals.
- **Public Awareness:** A lot of cybercrimes are successful because they take advantage of human weaknesses through social engineering, phishing, and hacking. Crime can be decreased by encouraging better cyber practices and increasing public knowledge of cyberthreats.

INDIA'S REGULATORY FRAMEWORK:

The goal of India's 2013 National Cyber Security Policy was to establish "a secure and resilient cyberspace for citizens, businesses, and Government."One The strategy acknowledged the dangers that cyberattacks pose to national security, the economy, and human life. The strategy also outlined important cyberspace security tactics, the majority of which are still relevant today. However, a new national cyber security policy is long necessary, especially since the current one is ten years old. In order to secure national cyberspace, the government announced in December 2022 that it had developed a draft cyber security plan.2. Nevertheless, the strategy's specifics and execution schedules were left out.

The Information Technology Act (the "IT Act") of 2000 Among other things, the IT Act stipulates penalties for offenses involving data or electronic communication as well as other offenses pertaining to cyber security. The offender may also be required to pay compensation for certain offenses, such as gaining access to computers, computer

systems, or computer networks without the owner's or person in charge's consent, downloading or copying data from computers, or denying access to computers.

Section 43 of the IT Act, which deals with computed related offenses, stipulates that compensation must be paid for specific actions involving computer infrastructure (such as computers, computer systems, and computer networks) and resources when they are taken without the owner or person in charge of them. This covers, among other things, illegal access, downloads, computer contamination, damage, and denial of access. If committed dishonestly or fraudulently, these acts are punished under Section 66 by up to three years in prison and/or a fine of up to INR 500,000. Furthermore, anyone who has obtained access to information about another person's personal details and divulges it without that person's consent with the knowledge or intent to cause him unlawful damage or unjust gain, is punishable by up to three years in prison and/or a fine of up to INR 500,000. altering source papers on computers, When computer source code must be stored or maintained in accordance with applicable laws, willful hiding, destruction, or alteration of such code is punishable by up to three years in prison and/or a fine of up to INR 200,000.

Keeping stolen resources or devices dishonestly: If someone receives or keeps a stolen electronic resource knowing that it is stolen, they could face up to three years in prison and/or a fine of up to INR 100,000.

Identity theft is when someone uses another person's password, electronic signature, or other distinctive identifying information fraudulently or dishonestly. It carries a maximum sentence of three years in prison and a maximum fine of INR 500,000.

impersonation with the use of a computer program, Cheating by utilizing a computer resource or electronic device to impersonate someone is punished by up to three years in prison and a fine of up to INR 100,000. The Indian Penal Code Although the IT Act lists particular offenses, there are other provisions in India's general criminal law that allow for remedy. Cybercrimes may be considered an offense under a number of IPC articles, including:

Deceiving someone to deliver property to someone that he would not have delivered normally if he had not been deceived is considered cheating. One example of a cybercrime would be tricking someone into sending private or restricted information to someone who isn't permitted to get it, something that the fooled individual would not have sent in the first place. electronic record forgery, According to this clause, an act pertaining to any electronic document is specifically mentioned, making it a felony. It involves creating a fraudulent document or electronic record that could harm someone else or even result in a fictitious property claim. If done with the intent to conduct such an act, it would be considered forgery and subject to a maximum sentence of two years in jail. A person who knowingly receives or retains stolen property—such as an electronic device—may face up to three years in jail, just like the IT Act offense.

Nonetheless, it is a well-established fact that a special law—in this case, the IT Act—takes precedence over a general law, such as the IPC.13. Therefore, only the IT Act may be used to prosecute someone with committing an offense if it is covered by both the IPC and the IT Act.

PROCEDURE FOR CYBERCRIME REPORTING AND PROSECUTION

After documenting the information, the police will either submit the offender to the magistrate or reduce it into a First Information report (or "FIR") 14 based on the type of offense (cognizable or non-cognizable). Following this, the police begin their investigation into the offense (or are instructed to do so by the magistrate16), and if the magistrate determines there is good grounds to do so, a criminal process is initiated.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

REGISTER COMPLAINT WITH NATIONAL CYBER CRIME REPORTING:

The National Cyber Crime Reporting Portal is the only way to report cybercrimes.18 As previously stated in Section 3(B)(i), the Indian government launched this facility to make it easier for victims and complainants to file online complaints about cybercrime. There are two ways to report cybercrimes through the portal: Report either (1) a crime involving women or children or (2) other cybercrimes. Cybersecurity-related offenses such ransomware, hacking, online financial frauds, cryptocurrency crimes, and online cyber trafficking, as described in the previous section, would be considered further cybercrimes. Although this platform allows all Indian nationals to report cybercrimes, the FAQs also mention that anyone who is not an Indian citizen but has been the victim of an internet crime can register a complaint. an Indian person or business.19. In India, more than 30 cities currently have their own cyber cells, and each town and village has its own dedicated cyber cell.

THE HE FUNCTION OF LAW ENFORCEMENT AND CYBERSECURITY EXPERTS

The role of cybersecurity and law enforcement professionals:

- **Investigating Cybercrimes:** The appropriate cybercrime units within law enforcement organizations look into and collect evidence of cybercrime. To combat cybercrime, they may work along with forensic divisions and cyber security divisions.
- **Response against Cybercrime:** The experts are in charge of identifying, evaluating, and reacting to cybercrime in government infrastructure and businesses, including malware assaults, data breaches, and cyberattacks.
- **Digital Forensics:** To assist with cybercrime investigations and prosecutions, forensic specialists analyze and extract evidence from digital devices, computer systems, and network traffic.
- **Cyber security Awareness:** Professionals in law enforcement and cyber security are essential in educating and training individuals, companies, and organizations on cybercrime prevention and best practices.
- **International Collaboration:** Cybercrime has no national boundaries. For the purpose of investigating and prosecuting cybercrime in various jurisdictions, law enforcement, cyber security, and legal branches must work together internationally and coordinate their efforts.

CASE STUDIES UNDER CYBER LAW

The landmark case studies under cyber law aren given below

i.ICICI Bank Phishing Case (2003):

In one instance, hackers imitated the ICICI Bank website using a phishing attack, fooling customers into disclosing their personal information and login credentials. It resulted in monetary losses for the user and harm to the bank's image. The event led to legal proceedings under the IT Act, with an emphasis on data theft and unauthorized access offenses.

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

Section 66A of the Information Technology Act, which was criticized for being unduly broad and vulnerable to abuse to restrict free speech, was challenged in this historic case. The Indian Supreme Court ruled that Section 66A was unconstitutional, highlighting the significance of protecting internet freedom of expression.

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

These cases brought to light problems with the online publication of court rulings and private case data. The court discussed the need for increased confidentiality and cyber security while handling court papers and rulings.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

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

The Karnataka Power Corporation Limited's systems were the subject of a ransomware assault. Financial losses and an interruption in power supply operations were the results. The risks of ransomware attacks on vital infrastructure were highlighted by the investigations that followed in order to find the criminals and deal with the criminality.

v. Data Breach at Air India (2021):

Millions of Air India passengers' private information was made public due to a serious data breach. They jeopardized the airline's reputation, compromised passenger data, and raised the possibility of identity theft. Under the IT Act's data protection rules, investigations were started, highlighting how crucial it is to secure personal information.

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

An essential digital certificate for online security communication was issued by Diginoter, a Dutch certificate authority (CA). Attackers infiltrated the Diginet system in 2011 and issued fake certificates, putting internet security and trust at risk. The Dutch Government assumed operational administration of Diginoter's system in September 2011 following the revelation that a security compromise had led to the fraudulent issuance of certificates. The business announced its bankruptcy in the same month.

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

North Korean hacker Park Jin Hyok belonged to the Lazarus group, a cybercrime organization run by the Korean government. In addition to stealing 81 million dollars from Bank of Bangladesh, Park Jin Hyok was responsible for the Wanna Cry ransomware assault in 2017 and the Sony Pictures hack in 2014. Park Jin Hyok was charged by the United States in September 2018 with computer fraud, digital abuse, identity theft, and wire fraud.

viii. Vietnam Case of Cyber espionage

Cyber spies from Vietnam are allegedly targeting Chinese government entities in an effort to obtain important information about the Covid-19 crisis. The hackers are collecting China's response to the COVID-19 epidemic on behalf of the Vietnamese government.(Fire Eye, publisher)

ix.Petya Ransomware

The ransomware strain known as Petya was initially discovered in 2016. Petya encrypted the victim's computer's files and data, just like other ransomware. Before they can decrypt the files and restore their use, Petya's activities require payment in Bit currencies. in contrast to certain older ransomware strains that blackmail the victim by encrypting only specific critical files. Petya makes it impossible to access any files on a computer's hard drive by locking up the entire disk, particularly when it encrypts the master file table. Only Windows-based PCs have been seen to be targeted by Petya.

x.Not Petya case

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

1. enhancing email security procedures. An infected email attachment was the initial step in the majority of Petya attacks and some non-Petya assaults. Organizations may stop this by blocking internal email attachments, scanning emails for malware, and teaching users not to click attachments they don't trust.
2. Regularly fixing vulnerabilities. Months before the attacks occurred, a patch for Not Petya's Eternal Blue exploit was ready. Generally speaking, ransomware attacks frequently take use of software flaws to either access a network or move laterally within it. These attack vectors can be eliminated with the aid of software updates and vulnerability patches.
3. Data and file backup. Cloud Flare One can also be adopted by organizations. It

is a platform that facilitates users' safe access to necessary resources. By employing a Zero Trust Security methodology,Cloud Flare aids in containing and preventing ransomware infections.

CONCLUSION

A new era of criminal activity, collectively referred to as cybercrime, has now been brought about by the digital age. These days, the internet and computer technology are constantly expanding. The complex realm of cybercrime was established by this study. Cybercrime comes in a variety of forms, and addressing these online dangers presents a number of difficulties. The problems are numerous and intricate, ranging from jurisdiction concerns and online anonymity to the necessity for international cooperation and the quickly changing nature of technology.

Although cyberattacks can come from anywhere in the world, it's frequently unclear who has jurisdiction over these crimes. Both the hacker and the victim are free to remain in different countries. Determining which laws apply and which authorities are authorized to conduct investigations and bring charges is extremely challenging. It is quite difficult to track down the origin of cyberattacks. Hackers can conceal their identities and the location of the crime with ease, making it difficult to identify the culprit. The threat of cybercrime is growing along with the digital landscape. The foundation of India's legal framework for preventing cybercrime and advancing cybersecurity is the Information Technology Act of 2000. To stay up with changing trends, it is crucial to update and reinforce cyber regulations on a regular basis.

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