The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBER CRIMES AND LEGAL REMEDIES

Subhadarsini Patra

INTRODUCTION

Cyber crime refers to illegal activities using computers, mobile phones,digital devices, or the internet. With the rapid growth of technologies, people increasingly use online platforms for education, banking, communication, and also other day to day activities. However, the increasing use of technology has also created new opportunities for criminals. There are various types of cyber Crimes and it includes online fraud, identity theft, hacking,cyber stalking, and also the misuse of personal information. In today's digital era, there are various forms of new cyber crimes that are raising serious concerns and these are deepfakes and technology-based frauds. One of the main difficulties in dealing with cyber crime is that the offenders can hide their true identity and also operate from different locations. Since cyber crimes can cross national and international boundaries, it can be difficult to trace the offenders. Therefore, it is very important to have strong laws, proper investigation, effective legal remedies, and also create public awareness to prevent and control cyber crimes.

MEANING AND NATURE OF CYBER CRIME

MEANING

The term cyber crime covers different types of unlawful activities involving computers, digital devices, and internet networks. In some cases, the main target is a computer or intent,

while in other cases, it is used as a tool to commit crimes. Cyber crime may be committed against an individual, financial institutions, or government organisations. Common examples include hacking, data theft, and online fraud.

NATURE

The nature of cyber crimes makes them different from traditional crimes because it involves digital technology and electronic evidence that can cross national borders. There are various nature and these are:

- Borderless: Cyber criminals can commit offences from one country while targeting another country.
- Anonymity: Criminals can hide their identity and location.
- Large-Scale impact: A single attack can affect many people or systems within a short period.
- Digital Evidence: Evidence such as messages, email, records, and files can be changed and deleted.
- Technical nature: Cyber crime often involves methods such as hacking, malware,phishing,or manipulation of users to get confidential information.

MAJOR TYPES OF CYBER CRIMES

There are various forms of cyber crimes. It can be divided according to the person, property, organization, and institutions targeted by the offender. Cyber crimes can cause financial loss, privacy violation, confidential harm, reputational harm, and also threat to public security. There are various types and these are:

1. Cyber Crimes Against Individuals:
   These crimes directly affect a
   person's safety, identity, privacy and
   or reputation.

- Identity theft: In this fraud it involves the unauthorised use of personal information such as Aadhaar details, and passwords to commit fraud .

- Cyber stalking and Harassment: In this type of cyber crime, the offender repeatedly follows and send unwanted or threatening message to a person through various online platforms
- Phishing and Social Engineering: Criminals use fake messages, emails, websites, and links to manipulate people into sharing their personal details.
- Online Defamation: False or harmful statements posted online may damage a person's personal information and reputation.

2. Cyber Crimes Against Property:
   These types of cyber crimes target
   digital information, computer system,
   money and also various other digital
   assets

2 Ransomware and Malware: Criminals use harmful software to damage, and block computer systems and also demand money to regain them.

3 Online Financial Fraud: Offenders may use fake payment links, stolen card details, and also various other methods to unlawfully obtain money.

4 Hacking and Unauthorized Access: In this type of fraud, criminals may enter computer systems, email accounts, and databases without the owner’s approval.

3. Cyber Crimes Against Government or the State:
   These crimes directly target
   government system, public
   infrastructure or national security.

2 Cyber Terrorism: Cyber attack may target important important public systems or infrastructure and also it may cause serious distribution

3 Cyber Espionage: In this type of cyber crime, criminals may gain unlawful access to government, military, or defence networks to collect confidential information.

4 Website Defacement: Criminals may enter government websites without authorization and also delete the information.

LEGAL FRAMEWORKS IN INDIA

India has various laws to prevent cyber crime and also safeguard people from the misuse of technology. These laws deal with cyber offence and also other crimes committed through computers, internet, and also mobile phone

1.**INFORMATION TECHNOLOGY ACT, 2000:** The Information Technology Act, 2000 is the main law to deal with cyber crimes in India. It provides various rules and also punishments for various different offences involving computer and digital system[1]

- Section 43: It covers unauthorised access, downloading data and causing damage to computer systems.[2]
- Section 66: It deals with computer-related offences committed dishonestly.[3]
- Section 66C: It covers identity theft involving the misuse of personal information.
- Section 66D: it includes cheating by impersonating another person using a computer.
- Section 66F: Deals with cyber Terrorism

2.**BHARATIYA NYAYA SANHITA, 2023**

The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal code from 1 July, 2024. It also applies in traditional offences such as cheating, forgery, or intimidation when they are committed using digital technology.[4]

3.**DIGITAL PERSONAL DATA PROTECTION ACT, 2023**

The Digital Personal Data Protection Act, 2023 provides rules for protection of digital Personal Data. It also provides certain responsibilities to organisations regarding the collection and handling of personal data.[5]

4.**CERT-IN**

The Indian Computer Emergency Response Team works under section 70B of the IT Act and it also plays a very important role in responding to cybersecurity incidents and also improving cyber security measures in India.

[1] Information Technology Act, 2000
[2] Information Technology Act, No. 21 of 2000, § 43
[3] Information Technology Act, No. 21 of 2000, § 66
[4] Bharatiya Nyaya Sanhita, 2023
[5] Digital Personal Data Protection Act, 2023

LEGAL REMEDIES AVAILABLE TO VICTIMS

Victims of cyber crime in India have several legal remedies and administrative measures to protect their rights. These measures also help in reporting offences, recovering losses and also taking action against offenders

2 Administrative Remedies: In cases of online financial fraud, victims should report the incident immediately by calling the 1930 Cyber Crime Helpline. Quick reporting can help the authorities and banks take steps to prevent further loss.[6]

3 Civil Remedies: victims who suffer losses because of data theft, misuse of personal information, and unauthorised access can seek compensation through the relevant legal authorities. Courts may also issue orders for removal of unlawful content in suitable cases.

4 Criminal Remedies: A victim can file a complaint with the local police station or a cyber crime cell. Depending on the nature of the offence, legal action may be taken under the Information Technology Act, 2000 and also the Bharatiya Nyaya Sanhita, 2023.

5 Banking and Consumer Remedies: Victims of unauthorised online transactions should immediately inform their bank and also report fraud. Consumers may also seek relief under consumer protection laws when they suffer losses because of unfair practice.

CHALLENGES IN COMBATING CYBER CRIMES

Although there are various laws to deal with cyber crimes, their prevention and investigation remain difficult. It creates various challenges for police and investigators.

- Cross-Border Nature: Cyber criminals can operate from one country and target people in another country. This makes investigation difficult because different countries have different procedures and it may be difficult to obtain information from another country.
- Anonymity of offenders: Cyber criminals may hide their true identity and location by using different online tools.

[6] Indian Cybercrime Coordination Centre, National Cyber Crime Reporting Portal, https://www.cybercrime.gov.in (last visited Sept. 28, 2026).

- Difficulty in collecting Digital Evidence: Digital Evidence including messages, emails, computer records, and transaction details can be easily changed and deleted. It is very important to collect and store digital evidence carefully because any kind of delay may lead to the loss of important information.
- Rapid Development of Technologies: Due to the rapid growth of new technology, criminals can also use new methods to commit crimes. Artificial Intelligence can be misused to create images and videos, which can make fraud.
- Lake of Skilled Personnel: Cyber crime investigations require trained police officers, forensic experts, and technical professionals. Because many agencies may not have trained professionals to properly deal with and investigate complex cyber crimes.
- Lack of Public Awareness: Many people are still not aware of common cyber threats such as phishing, fake links, online fraud, and identity theft. Lack of awareness can increase the risk of cyber crime. So awareness programs are very important to prevent cyber crime.

SUGGESTIONS

To effectively address cyber crimes in India, it needs various strong laws and greater investigation systems. There are various measures can help and these measures are:

- Update Cyber Laws: It is very important to regularly update Cyber Laws to address new forms of cyber crimes involving Artificial Intelligence, deepfake and other technologies.
- Established Specialised Cyber Courts: Specialised courts with trained judges can handle complex cyber crime cases more effectively.
- Strengthen International Cooperation: Since cyber criminals can operate across different countries, cooperation between countries is very important for effective investigation.
- Improve Digital Forensic: Police agencies should have proper forensic facilities and also use proper methods to collect, store and protect digital evidence.
- Increase Public Awareness: It is very important to organise awareness programmes to educate people about fishing, online fraud, and other common cyber threats.

CONCLUSION

With the rapid growth of technology, cyber crime is a serious challenge.Its borderless nature, hidden identities, changing methods, and also difficulty in handling digital evidence make investigation and prosecution difficult. Although India has various laws including the Information Technology Act, 2000 and Digital Personal Data Protection Act, to address cyber crime, it requires stronger investigation systems. With the advancement of new technologies, it is very important to update Cyber Laws. A combination of effective laws, trained investigators, reliable digital evidence, and public awareness can help protect individuals and organisations and also create a safe digital environment.