

Cyber Crime in India: Emerging Challenges, Legal Framework, Judicial Trends and Cybersecurity Concerns

Dr. Nidhi Sharma ✉

Associate Professor, Faculty of law, Agra college, Agra, Uttar Pradesh, India.

Due to the rapid growth of information and technology, the three main factors which have transformed were social, economic and administrative structure of modern-welfare society. There are multiple tools like the internet, smartphones including apps, digital banking including digital transactions, e-commerce, social media and digital governance which have become a part and parcel of everyday life. At the same time, increased dependence on digital infrastructure has created new opportunities for criminal activity. Cyber-crime has therefore emerged as an important area of contemporary criminal law and cybersecurity. Cyber-crimes differ from conventional crimes because computers and digital networks may function as the target, instrument or environment of the offence. Activities such as hacking, identity theft, phishing, ransomware, cyber stalking, online financial fraud and other related offences like data theft, cyber terrorism, digital arrest and publication of digital content which is unlawful and opposed to public policy has created a lot of challenges not only for individuals but also to NGO's, businesses and Government institutions. With respect to technology, the parent law created by the Parliament is IT Act of 2000 and other laws in support of this act are Bhartiya Nyaya Sanhita, 2023 and Digital Personal Data Protection Act of 2023. Both the acts have a vision to punish the offender's committing crime through digital technologies. The main vision of this paper is to examine the concept, nature, forms and extent of cyber-crime, and also to focus upon the judicial developments which have taken place including electronic evidence credibility and authenticity, challenges related to cyber-security, data protection and institutional mechanism. In order to gain proper control over cyber-crimes, it requires, coordination between criminal law, cybersecurity regulation, digital forensics, data protection, public awareness and international cooperation.

Keywords: IT Act of 2000, Bhartiya Nyaya Sanhita of 2023, Digital Arrest, Electronic Evidence, Cyber Crimes.

1. Introduction

Major transformation has been brought in by Information Technology which has altered the behavioral patterns of how individuals communicate, conduct business operations, access financial services including digital transactions and interaction with public institutions. Internet connectivity has enabled instantaneous communication and access to information across geographical boundaries. Digital payments, online banking, e-commerce and social-media platforms have further increased society's dependence upon digital infrastructure. Digital payments, online banking, e-commerce and social-media platforms have further increased society's dependence upon digital infrastructure. However, technological development has also resulted in the emergence of new forms of

criminality. Exploitation of computer systems, mobile and other technological devices, networks and online platforms for unlawful purposes. Unlike many traditional offences, cyber-crimes can be committed remotely, rapidly and across national borders.

Cyber-crime may affect individuals through identity theft, financial fraud, cyber stalking and online harassment. Businesses may face ransomware, industrial espionage, data theft and disruption of computer systems. Government institutions and critical infrastructure may become targets of cyber-attacks capable of affecting public services and national security.

The legal response to cyber-crime must therefore address two connected objectives: preventing and punishing unlawful

conduct while ensuring appropriate safeguards for privacy, freedom of expression, due process and other legal rights.

India's cyber-law framework has developed considerably since the enactment of the Information Technology Act, 2000. There were multiple legislative, judicial and institutional developments which have expanded the legal response against cyber-security violations and other digital offences.

2. Concept of Cyber Crime

There is no universally accepted single definition of cyber-crime. Cyber-crime refers to unlawful activities performed through technological intervention involving computer resource, communication networks, digital devices and apps and also includes electronic data which is the main driving force behind all the online crimes in the world.

When we talk about the use of a computer, it has multiple relationships with crime as in today's world, maximum of the crime committed is through digital means. There are three ways through which computer and crime are directly connected to each other:

-

- a. When Computer is the main target and the offender attacks the computer system as a whole or a network which consist of multiple data.
- b. Computer as the instrument – the offender uses technology to commit an otherwise recognizable offence.
- c. Computer as the environment – the digital environment facilitates or provides the setting for criminal conduct.

For example, unauthorized access to a server represents an attack upon a computer system. Online banking fraud uses digital technology as an instrument. Cyber stalking uses online communication platforms as an environment for unlawful conduct.

Cyber-crime can consequently include both offences specifically created by legislation and conventional offences committed through digital means.

3.Characteristics of Cyber Crimes

Cyber Crime possesses several characteristics that distinguishes it from many conventional offences.

3.1 Borderless Nature

An offender may operate from one country, use infrastructure located in another country and target a victim in the third country. This creates difficulty concerning jurisdiction and investigation.

3.2 Anonymity

Cyber Criminals conceal their identity through compromised accounts, anonymization services and other related techniques.

3.3 Speed of Commission

A cyber-attack can affect thousands or even millions of systems within a short period.

3.4 Volatile Evidence

Digital evidence can be deleted, modified, encrypted or overwritten. Consequently, preservation and forensic acquisition are important.

3.5 Low Physical Presence

Many cyber-crimes can be committed remotely without the offender physically entering the location of the victim.

3.6 Technological Complexity

To conduct proper investigation, specialized knowledge of malware, end to end encryption and other related viruses are required which includes cloud computing and digital forensics.

3.7 Cross-Border Investigation

If the servers or offenders are outside India then proper investigation can only be conducted if there is International Co-operation.

4. Major Forms of Cyber Crimes

4.1 Hacking and Unauthorized Access: -

Hacking generally refers to obtaining unauthorized access to a computer system, network or digital account. The main aim of unauthorized access is to steal information, manipulate the data against the disadvantage of the real originator and install malicious software to disrupt operations.

Section 43 of IT Act addresses specified acts involving access and damage to computer resources which is totally unauthorized. Section 66 of the concerned act talks about the punishment and criminal consequences which can occur if the acts mentioned under Section 43 are committed dishonestly or fraudulently.

4.2 Phishing

Phishing involves deceptive communications designed to induce individuals to disclose passwords, banking information, authentication codes or other sensitive information.

Modern phishing attacks may use apparently legitimate websites, emails, text

messages, social- media accounts or mobile applications. The problem is particularly significant because the attack may exploit human behavior rather than a technical vulnerability.

4.3 Identity Theft

Identity theft involves the unlawful use of another person's identifying information. Identity thefts digitally involve usernames, passwords, and identification documents, banking credentials or other personal information. Identity theft is addressed by Section 66 of It Act 2000.

4.4 Cheating by digital means

Online frauds involve false representation, fraudulent websites, fake investment opportunities, impersonation or manipulation of victims into transferring money. Depending upon the facts, provisions of general criminal law may also become relevant.

4.5 Cyber-Stacking and Online Harassment

Digital communication platforms can be misused for repeated monitoring, intimidation, threats or harassment. Cyber stalking can affect victims through social-media platforms, email, messaging applications and other digital channels.

The legal response may involve technology legislation as well as general criminal law, depending on the particular conduct.

4.6 Ransome Ware: -

Ransomware is a malicious software designed to restrict access to systems or data

commonly by end-to-end encryption, and demanding money from the victim through impersonation and digital arrest.

Ransomware can affect individuals, hospitals, educational institutions, companies and public bodies. The increasing digitisation of essential services makes ransomware a significant cybersecurity concern.

4.7 Data Theft

Un-Authorized acquisition of confidential or personal information can cause financial, reputational and privacy-related harm. Data theft may involve customer information, financial records, passwords, trade secrets, intellectual property or government information.

4.8 Cyber Terrorism

Cyber technology may be used to threaten national security, critical infrastructure or essential services. Section 66F of the Information Technology Act addresses cyber terrorism. Cyber terrorism must be distinguished from ordinary cyber offences because the relevant conduct may have severe implications beyond individual victims to National Sovereignty, security and integrity of India and public infrastructure.

5. Cyber Crime in India: Legal Framework

There are several laws and institutional mechanisms which showcases India's cybercrime framework. The principal legal instruments are as follows: -

- a. IT Act of 2000 which gives legal recognition to electronic evidence.
- b. IT rules and regulations

c. Bhartiya Nyaya Sanhita of 2023 which talks about the procedure.

d. Bharitya Sakshya Adhiniyam of 2023 which talks about evidences

e. Bharitya Nagarik Suraksha Sanhita of 2023

f. Other sector-specific regulatory frameworks.

6. Overview of IT Act Of 2000: -

IT Act of 2000 deals with e-records, digital signatures, e-evidences, e-transactions including bank transfers and UPI and several other computer related offences which has been discussed earlier. Important provisions include: -

a. Section 43 - Section 43 deals with various unauthorized acts involving computer systems and computer resources, including unauthorized access, downloading or copying data unlawfully which directly impacts and damages the computer systems and resource.

b. Section 43 A - Section 43A historically addressed compensation in specified circumstances which involves failure to implement security practices which are reasonable in relation to sensitive personal data or information available online.

c. Section 65: - Talks about the documents stored in a computer through online mode and tampering with the concerned documents.

d. Section 70 - Section 70 deals with protected systems.

e. Section 70B - Section 70B establishes the Indian Computer Emergency Response Team (CERT-In) as the national agency for responding to computer security incidents.

f. Section 75 - Section 75 provides for extra-territorial application in specified

circumstances involving conduct outside India.

g. Section 66F - Section 66F deals with offence related to cyber terrorism.

h. Section 66D - Section 66D addresses cheating by personation using a computer resource or a device used for communication.

7. BNS 2023 and Cyber Crime Doctrine

IPC 1860 was replaced by BNS 2023 and it is considered as the main procedural law of criminal jurisprudence in India. The importance of the BNS for cyber-crime lies partly in the fact that digital technology can be used to commit offences that are not exclusively technology-specific.

For example, deception, cheating, criminal intimidation, forgery, threats and other unlawful conduct may occur through electronic communication or digital platforms. IT Act of 2000 and other general criminal law principles shall be taken into consideration before conducting effective cyber-crime investigations.

The transition from IPC to BNS also makes it necessary for researchers and investigators to examine the corresponding statutory provisions under the new criminal-law framework.

8. Digital Personal Data Protection Act, 2023

It is one of the most important developments in India's data-protection framework. This law addresses the processing of digital personal data and establishes obligations concerning the protection of personal data. There is a directly proportional relationship between cyber-crime and data

protection of citizens which is particularly significant because cyber-attacks frequently involve unauthorized access to personal information.

In case of Data Breach, it can expose individuals to identity theft, financial fraud, impersonation and privacy violations.

9. Cybersecurity and cert-in Cert-

In is India's national agency for responding to computer security incidents under Section 70B of the Information Technology Act. Its functions include:

- a. Collection of information and its analysis related to cybersecurity incidents.
- b. Alerts and Advisories needs to be issued at regular intervals.
- c. Providing crucial information concerning cybersecurity practices.
- d. Awareness related to cybersecurity and its advantages and weaknesses.

The role of CERT-In demonstrates that cybercrime policy cannot be limited to criminal prosecution. Prevention, detection, incident response and technical coordination are equally important.

10. Cyber Crime and Electronic Evidence

Electronic evidence is central to many cybercrime investigations. Examples include:

- a. emails;
- b. crucial files saved in a computer.
- c. Data which is personal and saved in a mobile resource.
- d. CCTV recordings;
- e. digital photographs;
- f. social-media records;
- g. IP-related information;

- h. transaction records;
- i. metadata; and
- j. cloud-stored information

Digital Material is considered as authentic and credible if proper collection and preservation has taken place without compromising the authenticity. The new evidentiary framework therefore needs to be studied alongside cybercrime investigations.

10. Digital Forensic Sciences

Digital forensics is the process of identifying, collecting, preserving, examining and analyzing evidences collected through digital means. A forensic investigation may involve:

1. identification of relevant devices;
2. preservation of evidence;
3. forensic imaging;
4. recovery of deleted information;
5. analysis of system logs;
6. examination of malware;
7. analysis of network activity; and
8. preparation of forensic reports.

The authenticity of the electronic evidence is very crucial and important because digital evidences can easily be altered, compromised and deleted.

11. Jurisdictional Challenges

Jurisdiction represents one of the major challenges in cybercrime law. A single cyber offence may involve:

- ☐ an offender in one jurisdiction;
- ☐ a victim in another jurisdiction;
- ☐ a server in another country;

- ☐ payment processing through another country; and
- ☐ digital evidence stored on an international cloud platform.

Traditional territorial principles can therefore become difficult to apply.

12. Cyber Crime and Privacy

Cybersecurity measures must coexist with the protection of privacy. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognized right to privacy as a fundamental right under Article 21 of the Constitution. There is multiple personal information saved through online drive and platforms which needs proper constitutional protection and that is the reason right to privacy was declared a fundamental right.

Government surveillance, data collection, interception and cybersecurity measures must therefore operate within the constitutional and statutory framework.

13. Important Judicial Decisions

13.1 Shreya Singhal v. Union of India

In this judgement, the Hon'ble Supreme Court struck down Section 66 A of IT Act and declared it unconstitutional on the ground that Article 14, 19 and 21 is violated due to vague and inconsistent provisions.

This particular judgement is an important authority concerning the relationship between cyber regulation and fundamental rights.

13.2 Anvar P.V v. P.V Basher

Supreme Court laid down the evidentiary requirements related to the

electronic records under the existing evidence law. This judgement is the landmark judgement on admissibility of electronic evidence.

14. Cyber Crime and Financial Fraud

Digital financial transactions have increased convenience but have also created new avenues for fraud. Common methods include:

- fake customer-care numbers;
- phishing links;
- fraudulent investment schemes;
- impersonation;
- malicious mobile applications;
- un-authorized account access;
- payment-request scams; and
- social-engineering attacks.

Social Engineering is significant because the fraudsters are manipulating the innocent people to give/provide information or authorize a transaction which can directly impact the personal information of the victim. Therefore, cybersecurity awareness among users is an important component of cybercrime prevention.

15. Cyber Crime Against Women and Children

Multiple online abuse is taking place against women and children which is a very big cause of concern which requires concerted efforts and effective solutions. It includes: -

- Cyber Stalking
- cyber bullying;
- identity misuse;
- threats;

- Intimate Material dissemination without consent
- Online Sexual Exploitation
- Grooming
- harassment through social-media platforms.

Children require particular protection because of their age, vulnerability and increasing use of digital platforms.

16. Cyber Crime and Artificial Intelligence

Artificial intelligence is producing both beneficial cybersecurity applications and new risks. AI can assist organizations in detecting unusual network activity, identifying malware and analyzing large quantities of information related to security of India. There are criminals who use AI for multiple reasons:

- highly personalised phishing;
- automated social engineering;
- creation of deceptive content;
- impersonation;
- automated attacks; and
- manipulation of digital information.

The emergence of AI therefore creates a need for continuous development of cybersecurity policies and legal responses.

17. Challenges Before Law-Enforcement Agencies

Important challenges include:

17.1 Lack of Technical Expertise

Cyber investigations require specialized technical skills.

17.2 Shortage of Digital Forensic Infrastructure

Modern cyber investigations require sophisticated forensic laboratories and trained personnel.

17.3 Cross-Border Evidence

Obtaining electronic evidence from foreign jurisdictions may take considerable time.

17.4 Encryption

Strong encryption can create difficulties in accessing relevant evidence while simultaneously raising legitimate privacy concerns.

17.5 Rapid Technological Change

Law and investigative techniques can become outdated as technology develops.

17.6 Under-reporting

Some victims do not report cyber offences because of fear, embarrassment, uncertainty or lack of awareness.

18. Cyber Crime Reporting and Awareness

Public awareness plays an important role in preventing cyber-crime. Individuals should be encouraged to:

- Using strong and unique passwords which is very difficult to break.
- Multi-factor authentication to be activated for smooth functioning.
- avoid suspicious links;
- verify financial requests;
- update software;
- avoid installing applications from unknown sources;
- protect authentication credentials; and
- report suspected cyber-crime promptly.

India has established mechanisms for reporting cybercrime and promoting cyber-safety awareness.

19. International Legal Cooperation

Because cyber-crime frequently crosses national borders, international cooperation is essential. Important areas of cooperation include:

- preservation of electronic evidence;
- exchange of information;
- mutual legal assistance;
- extradition;
- investigation of cross-border financial crime;
- cooperation with technology companies; and
- development of common cybersecurity standards.

International cooperation remains particularly important where the offender, victim, infrastructure and evidence are located in different jurisdictions.

20. Findings

- The study indicates that cyber-crime is a rapidly evolving form of criminality that cannot be addressed exclusively through conventional criminal law.
- IT Act remains central to India's technology-specific cybercrime framework, while general criminal law may apply where digital technology is used to commit conventional offences.
- Electronic evidence is increasingly important in criminal investigations,

making digital-forensic capacity essential.

- Cyber-crime also has a strong connection with privacy and data protection because many attacks involve the unauthorized acquisition or misuse of personal information.
- Finally, technological prevention, public awareness and institutional coordination are necessary alongside criminal prosecution.

21. Suggestions

- Cybercrime investigation units should be strengthened at appropriate levels.
- Police officers, prosecutors and judicial officers should receive regular specialized training in cyber law and digital evidence.
- Digital forensic laboratories should be expanded and technologically upgraded.
- Mechanisms for rapid preservation of electronic evidence should be strengthened.
- International cooperation concerning cross-border cyber investigations should be improved.
- Public awareness programs concerning phishing, online fraud and identity theft should be expanded. Organizations handling personal data should adopt appropriate cybersecurity safeguards.
- Cybersecurity policies should be periodically reviewed in response to technological developments.

- Emerging risks associated with artificial intelligence, deepfakes and automated cyber-attacks should receive continuing legal and policy attention.

22. Conclusion

Cyber-crime represents one of the major legal challenges arising from the rapid development of digital technology. Its characteristics of anonymity, speed, technological complexity and cross-border operation create difficulties that are different from many traditional forms of criminality.

Nevertheless, legislation alone cannot eliminate cyber-crime. Effective prevention requires technological safeguards, skilled investigators, digital-forensic infrastructure, public awareness, institutional coordination and international cooperation. The continuing evolution of artificial intelligence, cloud computing, digital payments and other technologies means that cyber law must remain adaptable. A balanced approach should protect individuals and institutions from cyber threats while maintaining constitutional safeguards, privacy and due process. The future effectiveness of India's cybercrime framework will therefore depend upon the ability of law, technology and institutions to develop together.

References:

A. Primary Legal Sources

1. The Constitution of India, Government of India.
2. The Information Technology Act, 2000, Act No. 21 of 2000.

3. The Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023.
4. The Bharatiya Nagarik Suraksha Sanhita, 2023, Act No. 46 of 2023.
5. The Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023.
6. The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
7. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
8. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

B. Cases

1. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
2. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
5. State of Tamil Nadu v. Suhas Katti, 2004 Cri LJ 145.

C. Government and Institutional Sources

1. Ministry of Electronics and Information Technology, Government of India, Technology Act and Rules.
2. Indian Computer Emergency Response Team (CERT-In), Government of India,

Cybersecurity Advisories and Directions.

3. National Crime Records Bureau, Ministry of Home Affairs, Government of India, in India Reports.
4. National Cyber Crime Reporting Portal, Government of India.

5. Ministry of Home Affairs, Government of India, materials relating to cybercrime investigation and prevention.

D. International Sources

Crime:

1. Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.
2. United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime.
3. United Nations, materials concerning information and communications technology and cybercrime.

E. Books and Secondary Sources

1. Brenner, Susan W., Praeger. Cybercrime and the Law: Challenges of the New Millennium, Grabosky, Peter, Wall, David S., Press.
2. Electronic Crime, Prentice Hall. Cybercrime: The Transformation of Crime in the Information Age, Polity Yar, Majid, Cybercrime and Society, Sage Publications.
5. Furnell, Steven, Cybercrime: Vandalizing the Information Society, Addison-Wesley.

F. Important Online Legal Resources

- India Code – Legislative Department / Government of India.
- Ministry of Electronics and Information Technology (MeitY).
- Indian Computer Emergency Response Team (CERT-In).
- National Crime Records Bureau (NCRB).
- National Cyber Crime Reporting Portal.
- Supreme Court of India.
- United Nations Office on Drugs and Crime (UNODC).
- Council of Europe – Cybercrime Convention resources.