Cybercrime in India: Challenges of Law Enforcement, Investigation and Judicial Accountability

Submitted by:

Fateh Singh Saini

L.L.M. Student

University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

Under the Guidance of:

Dr. Navneet Kaur Chahal

Associate Professor

University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

ABSTRACT

The rapid advancement of information and communication technology has transformed modern society and created new opportunities for communication, business, education and governance. However, the increasing dependence on digital platforms has also resulted in the emergence of various forms of cybercrime, including identity theft, online financial fraud, cyberstalking, phishing, data breaches, cyber extortion and other technology-based offences. Cybercrime has become a significant challenge for the Indian criminal justice system because of its complex nature, anonymity, cross-border character and the difficulties associated with collecting and preserving electronic evidence.

The present research paper examines the challenges faced by law-enforcement agencies in preventing, detecting and investigating cybercrimes in India. It critically analyses the existing legal framework, particularly the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. Special attention is given to the role of cybercrime investigation agencies, digital forensic mechanisms, electronic evidence and the difficulties encountered by courts in determining the authenticity and admissibility of digital records.

Furthermore, the research explores the importance of judicial accountability in ensuring that cybercrime investigations are conducted fairly, transparently and in accordance with constitutional principles. It also examines the need to balance effective cybercrime prevention with fundamental rights, particularly the right to privacy, freedom of speech and the right to a fair trial. The paper concludes that although India has developed an important legislative and institutional framework to combat cybercrime, significant challenges remain in implementation, technological capacity, coordination and accountability. Strengthening forensic infrastructure, improving investigative expertise, ensuring procedural safeguards and promoting international cooperation are essential for developing an effective and rights-oriented cybercrime justice system.

Keywords: Cybercrime, Information Technology Act, Digital Evidence, Cyber Investigation, Law Enforcement, Judicial Accountability, Cyber Forensics, Right to Privacy, Criminal Justice System.

INTRODUCTION

The development of information technology has brought remarkable changes to the functioning of modern society. The internet has become an essential part of everyday life, facilitating communication, financial transactions, education, business operations and access to public services. Digital platforms have made human activities faster and more convenient, but they have simultaneously created new opportunities for criminal activities.

Cybercrime refers to unlawful activities committed through computers, digital devices, communication networks or the internet. Unlike traditional offences, cybercrimes may be committed without the physical presence of the offender at the location where the crime occurs. An individual sitting in one country may access the computer system of a victim located in another country, steal confidential information or conduct fraudulent financial transactions. This technological characteristic makes cybercrime particularly difficult to investigate and prosecute.1

In India, the expansion of digital banking, online shopping, social networking platforms, digital payment systems and electronic governance has increased the importance of cybersecurity and cybercrime regulation. Offences such as phishing, identity theft, online banking fraud, cyberstalking, ransomware attacks, data theft and the circulation of obscene or sexually explicit material have become significant concerns.2

The Indian Parliament enacted the Information Technology Act, 2000, as the principal legislation governing electronic transactions and several computer-related offences. The Act was subsequently amended in 2008 to address emerging technological developments and introduce provisions dealing with identity theft, cheating by personation, violation of privacy and cyber terrorism.3

However, the legal framework cannot be evaluated merely by examining the existence of statutory provisions. Its effectiveness also depends upon the ability of law-enforcement agencies to investigate offences, collect reliable digital evidence, identify offenders and ensure successful prosecution before competent courts.

One of the major difficulties in cybercrime investigation is the identification of offenders. Cybercriminals frequently use fake identities, encrypted communication, virtual private networks, anonymous accounts and foreign-based servers to conceal their activities. Digital evidence may also be deleted, altered, encrypted or transferred across different jurisdictions, creating additional difficulties for investigators.4

The introduction of the three new criminal laws in India has also brought important changes to the criminal justice framework. The Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 came into force on 1 July 2024. These legislations are particularly relevant to cybercrime

---

1 See Council of Europe, Convention on Cybercrime (Budapest Convention), 23 November 2001; United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (United Nations, 2013).

2 The Information Technology Act, 2000; Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C), official portal, https://i4c.mha.gov.in/.

3 The Information Technology Act, 2000, No. 21 of 2000, Preamble; see also the Information Technology (Amendment) Act, 2008, No. 10 of 2009.

4 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (United Nations, 2013), chs. 3–4.

because they address substantive criminal liability, criminal procedure and the treatment of electronic and digital evidence.5

Another important dimension is judicial accountability. Courts are responsible for ensuring that technological evidence is properly examined, constitutional rights are protected and criminal proceedings are conducted fairly. The judiciary must prevent misuse of investigative powers while ensuring that genuine cybercrime victims receive effective legal remedies.6

The present study therefore examines cybercrime in India from three interconnected perspectives: law enforcement, investigation and judicial accountability. It attempts to evaluate whether the existing legal and institutional framework is sufficiently effective to address the growing complexity of cyber offences.

Statement of the Research Problem

The increasing frequency and complexity of cybercrimes have exposed several weaknesses in the Indian criminal justice system. Although India has enacted legislation and established specialised institutions to address cyber threats, the practical enforcement of cyber laws continues to face difficulties.

Lack of specialised investigative personnel, inadequate digital forensic infrastructure, delays in obtaining electronic records, jurisdictional complications and difficulties in establishing the authenticity of electronic evidence affect the effectiveness of criminal proceedings.7

Furthermore, investigative authorities must exercise their powers within constitutional limitations. Unlawful searches, excessive surveillance, improper collection of personal information and violations of procedural safeguards may affect individual liberty and the fairness of criminal trials.8

The central research problem is whether the existing Indian legal framework adequately addresses these practical and constitutional challenges and whether stronger mechanisms of institutional and judicial accountability are required.

Objectives of the Study

1. To examine the meaning, nature and different forms of cybercrime in India.
2. To analyse the existing legal framework governing cybercrime and its enforcement.
3. To study the challenges faced by law-enforcement agencies during cybercrime investigations.
4. To examine the role of digital forensics and electronic evidence in criminal proceedings.
5. To analyse the role of the judiciary in ensuring accountability and protecting constitutional rights.
6. To identify the limitations of existing investigative and prosecutorial mechanisms.
7. To suggest legal and institutional reforms for strengthening India's response to cybercrime.

---

5 The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023; the Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023; and the Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023; all brought into force on 1 July 2024.

6 Constitution of India, arts. 14, 19 and 21; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

7 National Crime Records Bureau, Crime in India 2022 (Ministry of Home Affairs, Government of India), chapter on cyber crimes.

8 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

Research Methodology

The present research follows a doctrinal method of legal research. It is primarily based on secondary sources, including statutory provisions, judicial decisions, government publications, books, research articles, legal journals and reports relating to cybercrime and cybersecurity. The study analyses the relevant provisions of Indian legislation and examines judicial decisions dealing with privacy, electronic evidence, freedom of expression and procedural fairness. A critical and analytical approach has been adopted to evaluate the effectiveness of the existing legal framework and identify areas requiring reform.

CONCEPTUAL UNDERSTANDING OF CYBERCRIME

Meaning and Definition of Cybercrime

Cybercrime may broadly be understood as any unlawful activity in which a computer, computer system, computer network or digital communication device is used as a tool, target or medium of committing an offence. The term does not refer to a single category of criminal activity. Instead, it includes several offences that exploit digital technology to cause financial loss, obtain confidential information, violate privacy, threaten individuals or disrupt computer systems.9

Cybercrime may be directed against individuals, businesses, financial institutions, government departments and even national security infrastructure. Unlike conventional offences, cybercrimes are often characterised by anonymity, speed, technological sophistication and the ability to affect victims across geographical boundaries.

Nature and Characteristics of Cybercrime

Anonymity of offenders: Cybercriminals frequently use false identities, anonymous accounts and other technological methods to conceal their actual identity. This makes identification and prosecution difficult.

Borderless nature: Cyber offences may involve victims, offenders, servers and financial intermediaries situated in different countries. Consequently, determining jurisdiction becomes complicated.10

Volatility of digital evidence: Electronic evidence can be deleted, modified, overwritten or transferred within a short period. Investigators must therefore preserve digital information immediately and maintain its integrity.11

Technological sophistication: Cybercriminals continuously adopt advanced technologies, including encryption, malicious software, automated attacks and artificial intelligence, to commit offences.

Large-scale impact: A single cyberattack may affect thousands of individuals, organisations or computer networks simultaneously.

Difficulty in attribution: Establishing the connection between a particular device, digital account and actual offender requires technical investigation and corroborative evidence.

---

9 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (United Nations, 2013), pp. 11–15.

10 Council of Europe, Convention on Cybercrime (Budapest Convention), 23 November 2001, arts. 22 and 23.

11 See Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Academic Press, 2011).

Major Forms of Cybercrime in India

Phishing: Phishing involves fraudulent communications designed to deceive individuals into revealing confidential information such as passwords, banking details and authentication credentials.12

Identity Theft: Identity theft involves the unauthorised use of another person's electronic signature, password or other unique identification information. Section 66C of the Information Technology Act, 2000, specifically addresses identity theft.13

Cyberstalking and Online Harassment: Cyberstalking involves repeated unwanted online communication, monitoring, threats or harassment through digital platforms. Depending upon the facts, relevant provisions of the Bharatiya Nyaya Sanhita, 2023, and other applicable laws may be attracted.14

Online Financial Fraud: It includes fraudulent banking transactions, UPI fraud, credit card fraud, investment scams and deceptive online payment requests.

Data Theft and Data Breaches: These offences involve unauthorised access to confidential personal, commercial or government information.

Ransomware Attacks: Ransomware is malicious software that restricts access to computer systems or encrypts data and demands payment for restoring access.

Cyber Terrorism: Cyber terrorism involves the use of computer resources to threaten national security, sovereignty, integrity or other interests protected under law. Section 66F of the Information Technology Act, 2000, deals with cyber terrorism.15

Online Sexual Exploitation: Digital platforms may be misused for the circulation of obscene material, sexually explicit content, child sexual abuse material and other forms of online exploitation. Such offences may attract provisions of the Information Technology Act and other applicable criminal statutes.

Cybercrime and Traditional Crime: A Conceptual Distinction

Traditional crimes are generally associated with physical conduct, identifiable locations and direct interaction between the offender and victim. Cybercrimes, on the other hand, are frequently committed through digital networks without requiring physical proximity.

Basis	Traditional Crime	Cybercrime
Medium	Physical environment	Digital environment
Identification	Often based on physical clues	Requires digital attribution
Evidence	Physical objects and witnesses	Electronic records and digital traces
Jurisdiction	Generally territorial	May involve multiple jurisdictions

12 The Information Technology Act, 2000, ss. 43 and 66; see also Indian Cyber Crime Coordination Centre, National Cyber Crime Reporting Portal, https://cybercrime.gov.in/.

13 The Information Technology Act, 2000, s. 66C.

14 The Bharatiya Nyaya Sanhita, 2023, s. 78; see also the Information Technology Act, 2000, as applicable to the facts of a particular case.

15 The Information Technology Act, 2000, s. 66F.

Investigation	Conventional police methods	Technical and forensic methods
Speed	Often limited by physical circumstances	Can occur almost instantly

This distinction demonstrates why conventional investigative methods alone are insufficient to address modern cyber offences.

Evolution of Cybercrime Regulation in India

India's legal response to cybercrime developed alongside the expansion of computer networks and electronic commerce. The Information Technology Act, 2000, was enacted to provide legal recognition to electronic records and electronic transactions and to address certain computer-related offences.16

The Information Technology (Amendment) Act, 2008, significantly expanded the legal framework by introducing provisions relating to identity theft, cheating by personation, violation of privacy, cyber terrorism and sexually explicit electronic content.17

Subsequently, the development of specialised agencies, cybercrime reporting mechanisms and digital forensic facilities strengthened the institutional response. The enactment of the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 further transformed the criminal justice framework with effect from 1 July 2024.

These developments demonstrate that cybercrime regulation in India is an evolving process requiring continuous legal and technological adaptation.

LEGAL FRAMEWORK GOVERNING CYBERCRIME IN INDIA

India has developed a combination of substantive criminal laws, procedural laws, evidentiary provisions and institutional mechanisms to regulate cybercrime. The effectiveness of these laws depends upon their proper implementation and coordination among investigating authorities, forensic experts, prosecutors and judicial institutions.

Information Technology Act, 2000

The Information Technology Act, 2000, is the principal legislation dealing with electronic transactions, computer-related offences and certain aspects of cybersecurity in India. The Act was enacted to provide legal recognition to electronic records and electronic communication and to establish a legal framework for addressing offences involving computer systems and digital networks.18

Section 43 – Penalty and Compensation for Damage to Computer Systems: This provision deals with unauthorised access, downloading of information, introducing computer contaminants, damaging computer systems and other specified acts. It provides for compensation to affected persons.19

Section 65 – Tampering with Computer Source Documents: This section penalises the intentional concealment, destruction or alteration of computer source code required to be maintained by law.

16 The Information Technology Act, 2000, No. 21 of 2000.

17 The Information Technology (Amendment) Act, 2008, No. 10 of 2009.

18 The Information Technology Act, 2000, ss. 1–2 and 43–75.

19 The Information Technology Act, 2000, s. 43.

Section 66 – Computer-Related Offences: This provision criminalises acts referred to under Section 43 when committed dishonestly or fraudulently.

Section 66C – Identity Theft: It penalises the fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature.20

Section 66D – Cheating by Personation Using Computer Resources: This provision addresses cheating through personation by means of communication devices or computer resources.21

Section 66E – Violation of Privacy: It penalises capturing, publishing or transmitting images of the private area of a person without consent under the circumstances specified in the provision.

Section 66F – Cyber Terrorism: This provision deals with serious cyber activities intended or likely to threaten the unity, integrity, security or sovereignty of India or strike terror in people, subject to the statutory requirements.22

Section 67 – Publishing or Transmitting Obscene Material in Electronic Form: It penalises the publication or transmission of obscene material in electronic form.

Section 69 – Power to Issue Directions for Interception, Monitoring or Decryption: It provides the statutory framework for specified interception, monitoring or decryption directions, subject to legal conditions and safeguards.23

Section 70B – Indian Computer Emergency Response Team (CERT-In): This provision recognises CERT-In as the national agency for responding to cybersecurity incidents and performing related functions.24

Section 75 – Act to Apply for Offences or Contraventions Committed Outside India: It provides for the extraterritorial application of the Act in specified circumstances where an offence or contravention involves a computer, computer system or computer network located in India.25

Despite these provisions, effective enforcement remains challenging because cyber offences frequently involve technological complexity, multiple jurisdictions and difficulties in obtaining reliable electronic evidence.

Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS), replaced the Indian Penal Code, 1860, with effect from 1 July 2024. Although the Information Technology Act primarily addresses computer-related offences, the BNS is also relevant where digital platforms are used to commit conventional criminal offences.26

---

20 The Information Technology Act, 2000, s. 66C.

21 The Information Technology Act, 2000, s. 66D.

22 The Information Technology Act, 2000, s. 66F.

23 The Information Technology Act, 2000, s. 69; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

24 The Information Technology Act, 2000, s. 70B; CERT-In, Directions under s. 70B(6) of the Information Technology Act, 2000, 28 April 2022.

25 The Information Technology Act, 2000, s. 75.

26 The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023.

For example, online financial deception may attract the provisions relating to cheating, depending upon the facts. Forgery-related offences may arise where electronic records or digital documents are dishonestly fabricated. Criminal intimidation, stalking and other offences may also involve the misuse of digital communication.

The BNS therefore supplements the Information Technology Act by providing substantive criminal liability for various offences committed through digital means. However, the application of these provisions must be determined according to the ingredients of the particular offence and the facts established during investigation.

Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), replaced the Code of Criminal Procedure, 1973, with effect from 1 July 2024. It establishes the procedural framework for investigation, arrest, search, seizure, inquiry and trial.27

- Investigation of offences involving digital devices and electronic records.
- Collection and preservation of relevant information during criminal investigations.
- Search and seizure of devices and other material connected with offences.
- Recording of statements and use of electronic means in specified procedural circumstances.
- Ensuring procedural safeguards during investigation and trial.

The BNSS also provides a framework for electronic processes in criminal proceedings. Nevertheless, the practical implementation of these provisions requires trained personnel, appropriate technical infrastructure and proper procedural compliance.

Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), replaced the Indian Evidence Act, 1872, and came into force on 1 July 2024. The legislation is particularly important in cybercrime cases because electronic and digital records frequently constitute the primary evidence.28

Section 61: Recognises the legal effect, validity and enforceability of electronic or digital records, subject to the statutory framework.29

Section 62: Provides special provisions concerning evidence relating to electronic records.

Section 63: Prescribes the conditions and requirements governing the admissibility of electronic records produced as computer outputs.30

The BSA provides an important legal foundation for the use of digital evidence in criminal trials. However, admissibility alone does not establish the truthfulness or reliability of electronic information. Courts must also examine authenticity, integrity, source, chain of custody and the circumstances in which the record was obtained.

27 The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023.

28 The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023.

29 The Bharatiya Sakshya Adhiniyam, 2023, s. 61.

30 The Bharatiya Sakshya Adhiniyam, 2023, s. 63.

CERT-In and Its Role in Cybersecurity

The Indian Computer Emergency Response Team (CERT-In) functions under Section 70B of the Information Technology Act, 2000. It plays an important role in responding to cybersecurity incidents, issuing alerts, coordinating responses and disseminating information concerning cyber threats.31

The CERT-In Directions dated 28 April 2022 prescribe specified cybersecurity incident-reporting and information-retention requirements for covered entities. They are intended to improve the ability of authorities to analyse and respond to cybersecurity incidents.32

CERT-In is an important part of India's cybersecurity infrastructure. However, its technical incident-response functions must be distinguished from the criminal investigation and prosecution functions performed by competent law-enforcement authorities.

Institutional Framework for Combating Cybercrime

Indian Cyber Crime Coordination Centre (I4C): Established under the Ministry of Home Affairs, I4C aims to coordinate efforts to combat cybercrime and support law-enforcement agencies.33

National Cyber Crime Reporting Portal: The portal enables citizens to report cybercrime incidents, including offences involving women and children.34

Cyber Crime Helpline 1930: This helpline provides assistance in reporting financial cyber fraud and facilitating timely action to prevent the transfer of fraudulently obtained funds.

National Crime Records Bureau (NCRB): NCRB collects and publishes crime-related statistics, including information concerning cybercrime cases.35

State Cyber Crime Police Stations: These specialised units investigate cyber offences and provide technical assistance in dealing with digital evidence.

Cyber Forensic Laboratories: These laboratories assist investigating authorities through the examination of electronic devices, recovery of digital information and technical analysis of electronic records.

These institutions collectively contribute to India's cybercrime response. However, effective coordination between central agencies, state police, financial institutions, service providers and forensic experts remains essential.

CHALLENGES FACED BY LAW-ENFORCEMENT AGENCIES IN INDIA

Law-enforcement agencies are responsible for preventing, detecting and investigating criminal activities. However, cybercrime presents challenges that are substantially different from those encountered in conventional criminal investigations.

---

31 The Information Technology Act, 2000, s. 70B.

32 Indian Computer Emergency Response Team (CERT-In), Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents, 28 April 2022.

33 Ministry of Home Affairs, Government of India, Indian Cyber Crime Coordination Centre (I4C), https://i4c.mha.gov.in/.

34 Government of India, National Cyber Crime Reporting Portal, https://cybercrime.gov.in/.

35 National Crime Records Bureau, Crime in India 2022 (Ministry of Home Affairs, Government of India).

Lack of Technical Expertise: One of the major difficulties faced by investigating authorities is the shortage of personnel possessing specialised knowledge of cybersecurity, digital forensics, network analysis and electronic evidence examination. A shortage of trained personnel may result in delays, improper collection of evidence and difficulties in identifying offenders.

Anonymity and Identification of Cybercriminals: Cybercriminals frequently use fake accounts, encrypted communication platforms, proxy servers and other technological methods to conceal their identities. The identification of an offender may require the examination of IP addresses, login records, device information, transaction histories and communication records. Investigators must rely on multiple sources of evidence rather than treating a single digital identifier as conclusive proof.

Jurisdictional Challenges: Cybercrime frequently involves different geographical locations. The offender may operate from one country, use servers located in another country and target a victim residing in India. This creates questions concerning territorial jurisdiction, applicable laws, investigation powers and international cooperation. Although Section 75 of the Information Technology Act provides for extraterritorial application in specified circumstances, practical difficulties remain in obtaining information from foreign service providers and securing international assistance.36

Difficulty in Collection and Preservation of Digital Evidence: Digital evidence is highly vulnerable to alteration, deletion and destruction. Investigators must ensure that electronic devices are handled carefully and that appropriate forensic procedures are followed. The preservation of metadata, creation of forensic images, maintenance of hash values and documentation of the chain of custody are important for establishing the integrity of digital evidence.37

Lack of Adequate Cyber Forensic Infrastructure: Cyber forensic laboratories play a crucial role in identifying, recovering and analysing electronic information. Effective forensic examination requires advanced equipment, specialised software, trained experts and adequate financial resources. Inadequate infrastructure and delays in forensic examination may affect the timely completion of investigations and criminal trials.

Underreporting of Cybercrime: Many victims hesitate to report cybercrime because of embarrassment, fear of reputational damage, lack of awareness or the belief that reporting will not result in effective action. Underreporting affects the availability of reliable data and makes it difficult for authorities to identify patterns and develop effective prevention strategies.

Coordination Between Agencies: Cybercrime investigations may require cooperation between local police, specialised cyber units, central agencies, banks, internet service providers, social media companies and foreign authorities. The absence of effective coordination may delay access to information and complicate investigations.

DIGITAL EVIDENCE AND CHALLENGES IN CYBERCRIME INVESTIGATION

Digital evidence has become one of the most important components of modern criminal investigations. In cybercrime cases, the prosecution frequently depends upon electronic records to establish the identity of the offender, the nature of the offence and the connection between the accused and the criminal activity.

36 The Information Technology Act, 2000, s. 75; Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.

37 Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Academic Press, 2011).

Meaning of Digital Evidence

Digital evidence refers to information stored, transmitted or generated through electronic devices and digital systems that may be relevant to legal proceedings. It may include:38

- Emails and electronic messages.
- Social media conversations.
- Photographs and video recordings.
- Computer files and documents.
- Internet browsing records.
- IP address and server logs.
- Banking and online payment records.
- Mobile phone data and location-related records.
- Metadata and other technical information.

The evidentiary value of such material depends upon its authenticity, relevance, integrity and compliance with applicable legal requirements.

Importance of Digital Forensics

Digital forensics is the scientific process of identifying, collecting, preserving, examining and presenting electronic information for investigative or judicial purposes. It assists investigators in recovering deleted information, analysing electronic devices, identifying suspicious activities and reconstructing the sequence of events.39

8. Identification of potential sources of electronic evidence.
9. Preservation of devices and relevant electronic information.
10. Acquisition of forensic copies using appropriate procedures.
11. Examination and analysis of the collected material.
12. Documentation of findings and maintenance of chain of custody.
13. Preparation of forensic reports for use in legal proceedings.

The use of recognised forensic procedures is essential to protect the integrity of evidence and prevent allegations of tampering.

Chain of Custody

Chain of custody refers to the chronological documentation of the collection, handling, transfer, storage and examination of evidence. In cybercrime investigations, maintaining the chain of custody is particularly important because electronic information can be modified without visible physical changes.40

Investigators must document who collected the device, when it was collected, how it was stored, who accessed it and what forensic procedures were performed. Proper documentation helps courts evaluate whether the evidence remained intact throughout the investigative process.

38 Bharatiya Sakshya Adhiniyam, 2023, ss. 2(1)(d), 61–63.

39 National Institute of Standards and Technology, Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86 (2006).

40 Association of Chief Police Officers, Good Practice Guide for Digital Evidence, 5th ed. (2012), principles 1–4.

Admissibility of Electronic Evidence

The Bharatiya Sakshya Adhiniyam, 2023, recognises electronic and digital records as evidence and provides a statutory framework for their admissibility. Section 63 is particularly important because it lays down requirements for proving electronic records produced as computer outputs.41

The courts must examine whether the statutory conditions have been satisfied and whether the evidence is sufficiently reliable to be considered in the proceedings. It is equally important to distinguish between the admissibility of evidence and the weight that should be assigned to it. A digital record may satisfy the legal requirements for admission but still require careful evaluation regarding its accuracy, source and credibility.

Challenges Relating to Digital Evidence

- Alteration or manipulation of electronic records.
- Difficulty in recovering deleted or encrypted information.
- Inadequate forensic documentation.
- Delays in obtaining records from service providers.
- Difficulty in authenticating social media accounts.
- Lack of technical understanding among stakeholders.
- Cross-border storage of digital information.

These challenges demonstrate the need for specialised forensic training and uniform standards for handling electronic evidence.

JUDICIAL ACCOUNTABILITY IN CYBERCRIME CASES

Judicial accountability is an essential element of the criminal justice system. Courts must ensure that the investigation, prosecution and adjudication of cybercrime cases comply with the Constitution and applicable statutory provisions. The judiciary performs a dual function: it ensures that offenders are held accountable and protects individuals from arbitrary or unlawful exercise of investigative powers.

Role of the Judiciary in Cybercrime Adjudication

The judiciary plays an important role in determining the legality and reliability of evidence produced during cybercrime proceedings. Courts must examine whether digital records have been obtained lawfully, whether their authenticity has been established and whether the accused has been provided a fair opportunity to challenge the prosecution's evidence.42

Protection of Fundamental Rights

Cybercrime investigations may involve access to personal devices, electronic communications, financial information and private digital records. Such investigative activities must comply with constitutional safeguards. Article 21 protects life and personal liberty, Article 19 protects specified freedoms, including freedom of speech and expression subject to constitutionally permissible restrictions, and Article 14 ensures equality before the law.43

Judicial Accountability and Fair Trial

A fair trial requires that the prosecution establish its case through legally admissible and reliable evidence. In cybercrime cases, the accused must have an adequate opportunity to examine the electronic records relied upon by the

41 The Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63.

42 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

43 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

prosecution and challenge their authenticity. Courts should carefully assess forensic reports, expert opinions and technical evidence instead of accepting them without independent judicial scrutiny.44

Judicial Oversight of Investigative Powers

Law-enforcement agencies possess statutory powers to investigate offences, search premises, seize devices and obtain specified electronic information. However, these powers are not unlimited. Courts must ensure that investigative authorities act within the limits of the law and comply with applicable procedural safeguards.45

Problems Affecting Judicial Efficiency

The adjudication of cybercrime cases may be affected by lack of specialised technical knowledge, delays in receiving forensic reports, large volumes of electronic evidence, difficulty in understanding complex technological processes, shortage of specialised training for legal professionals and problems concerning cross-border evidence.

IMPORTANT JUDICIAL DECISIONS RELATING TO CYBERCRIME, DIGITAL EVIDENCE AND CONSTITUTIONAL RIGHTS

Shreya Singhal v. Union of India (2015)
Citation: (2015) 5 SCC 1.

The Supreme Court struck down Section 66A of the Information Technology Act, 2000, as unconstitutional because its vague and overbroad restrictions violated Article 19(1)(a) of the Constitution. The Court also considered the constitutional validity of other provisions relating to online content and intermediary liability.46

Significance: The judgment established that regulation of online activities must comply with constitutional guarantees. It also demonstrated the importance of protecting freedom of expression while addressing unlawful online conduct.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)
Citation: (2017) 10 SCC 1.

A nine-judge Constitution Bench of the Supreme Court unanimously recognised the right to privacy as a fundamental right protected under the Constitution. The Court explained that privacy is closely connected with dignity, autonomy and personal liberty.47

Significance: The judgment is highly relevant to cybercrime investigations because digital investigations frequently involve personal information, electronic communications and private data. Investigative powers must therefore comply with constitutional standards.

Anvar P.V. v. P.K. Basheer (2014)
Citation: (2014) 10 SCC 473.

The Supreme Court examined the requirements governing the admissibility of electronic records under the Indian Evidence Act, 1872. The Court emphasised the importance of complying with Section 65B when relying upon electronic records in the form of computer outputs.48

---

44 Constitution of India, arts. 14, 21 and 22; see also Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

45 Bharatiya Nagarik Suraksha Sanhita, 2023; Constitution of India, art. 21.

46 Shreya Singhal v. Union of India, (2015) 5 SCC 1.

47 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Significance: The decision established an important evidentiary framework for electronic records. Its historical significance must now be read alongside the applicable provisions of the Bharatiya Sakshya Adhiniyam, 2023.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)
Citation: (2020) 7 SCC 1.

The Supreme Court clarified the law relating to the certificate requirement under Section 65B of the Indian Evidence Act, 1872. The Court reaffirmed the importance of the certificate for the admissibility of electronic records produced as computer outputs, subject to the principles explained in the judgment.49

Significance: The decision highlighted that electronic evidence must satisfy prescribed evidentiary requirements before being relied upon in judicial proceedings. Its principles provide important historical guidance when examining the corresponding framework under Section 63 of the BSA, 2023.

People's Union for Civil Liberties v. Union of India (1997)
Citation: (1997) 1 SCC 301.

The Supreme Court examined the constitutional safeguards governing telephone interception and recognised the importance of procedural protections against arbitrary interference with privacy.

Significance: Although the case concerned telephone interception rather than cybercrime specifically, its principles are relevant to digital surveillance, interception of communications and the protection of personal liberty during investigations.

State of Tamil Nadu v. Suhas Katti (2004)
Citation: Early reported cybercrime prosecution under the Information Technology Act.

The case concerned the publication of obscene and defamatory messages concerning a woman through an online platform.

Significance: The case demonstrated the application of Indian cybercrime legislation to online harassment and highlighted the importance of electronic records in establishing criminal liability.

CRITICAL ANALYSIS AND MAJOR GAPS IN THE EXISTING LEGAL FRAMEWORK

Despite the development of statutory provisions and institutional mechanisms, the Indian cybercrime framework continues to face several implementation-related limitations.

Gap between legislation and implementation: The existence of comprehensive statutory provisions does not automatically guarantee effective enforcement. Investigative agencies require technical expertise, adequate resources and institutional coordination.

Rapid technological developments: Criminal activities involving artificial intelligence, deepfakes, cryptocurrency and sophisticated cyberattacks create new challenges that require continuous legal and regulatory adaptation.

Inadequate forensic capacity: The availability of trained digital forensic experts and modern forensic facilities remains essential for the effective examination of electronic evidence.

Delays in criminal proceedings: Delayed investigations, forensic examination and trials may weaken prosecution and adversely affect victims.

48 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

49 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

Privacy and surveillance concerns: The need to investigate cybercrime must be balanced against the constitutional right to privacy and the requirement of lawful and proportionate investigative action.

Limited international cooperation: Obtaining evidence from foreign jurisdictions may involve lengthy procedures and differences in legal systems, creating obstacles to effective prosecution.

Need for greater judicial specialisation: Courts must possess sufficient technological understanding to evaluate complex digital evidence and distinguish reliable forensic findings from unsupported technical claims.

The major concern is therefore not merely the absence of legal provisions but the gap between legal standards and their practical enforcement.

SUGGESTIONS AND RECOMMENDATIONS

To strengthen India's response to cybercrime, the following measures may be considered:

Strengthening Cybercrime Police Units: Specialised cybercrime units should be strengthened through recruitment, technical training and adequate investigative resources.

Improving Digital Forensic Infrastructure: Modern forensic laboratories should be established and upgraded to ensure timely examination of electronic devices and digital records.

Specialised Training for Judicial Officers: Judges, prosecutors and legal professionals should receive regular training in cyber law, digital forensics and electronic evidence.

Standardised Evidence Collection Procedures: Uniform procedures should be developed for the collection, preservation, examination and presentation of digital evidence.

Strengthening International Cooperation: India should improve coordination with foreign law-enforcement agencies and international institutions to address cross-border cyber offences.

Improving Public Awareness: Awareness campaigns should educate citizens about phishing, online financial fraud, identity theft, cyberstalking and safe digital practices.

Strengthening Institutional Coordination: Better coordination should be developed among state police, central agencies, banks, financial institutions and technology service providers.

Ensuring Privacy Protection: Investigative powers involving personal data and digital communications should be exercised according to the law and constitutional safeguards.

Improving Victim Support Mechanisms: Victims should receive accessible reporting facilities, timely assistance and appropriate legal remedies.

Continuous Legal Reform: Cyber laws should be reviewed periodically to address technological developments while maintaining constitutional protections and procedural fairness.

CONCLUSION

Cybercrime has emerged as one of the most significant challenges confronting India's modern criminal justice system. The rapid development of digital technology has transformed the nature of criminal activities and created new difficulties for law-enforcement agencies, investigators and judicial institutions. The borderless nature of cyberspace, anonymity of offenders, technological sophistication and volatility of electronic evidence make cybercrime fundamentally different from many traditional offences.

India has established an important legal framework through the Information Technology Act, 2000, along with the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam,

2023. These legislations provide the foundation for addressing computer-related offences, conducting criminal investigations and admitting electronic records in judicial proceedings. Institutions such as CERT-In, the Indian Cyber Crime Coordination Centre and the National Cyber Crime Reporting Portal also contribute to the prevention and response mechanisms.

However, the effectiveness of these legal measures depends upon their implementation. Shortages of technically trained investigators, inadequate forensic infrastructure, difficulties in preserving digital evidence, jurisdictional complications and delays in criminal proceedings continue to affect the successful prosecution of cyber offences.

The judiciary has an equally significant responsibility in this regard. It must ensure that electronic evidence is properly evaluated, investigative powers are exercised lawfully and the constitutional rights of individuals are protected. The principles established in Shreya Singhal v. Union of India and Justice K.S. Puttaswamy v. Union of India demonstrate that the fight against cybercrime must remain consistent with freedom of expression, privacy and personal liberty.

It is therefore necessary to adopt a comprehensive approach that combines effective legislation, technological advancement, institutional coordination and judicial accountability. Strengthening cyber forensic capabilities, providing specialised training, improving international cooperation and ensuring timely investigation and adjudication can significantly improve the effectiveness of India's cybercrime framework.

Ultimately, the objective of cybercrime regulation should not merely be the punishment of offenders but also the protection of citizens, preservation of constitutional values and maintenance of public confidence in the criminal justice system. A technologically capable, transparent and accountable legal system is essential to ensure justice in the digital era.

BIBLIOGRAPHY

Statutes and Legislation

1. The Constitution of India, 1950.
2. The Information Technology Act, 2000.
3. The Information Technology (Amendment) Act, 2008.
4. The Bharatiya Nyaya Sanhita, 2023.
5. The Bharatiya Nagarik Suraksha Sanhita, 2023.
6. The Bharatiya Sakshya Adhiniyam, 2023.
7. The Digital Personal Data Protection Act, 2023.
8. The Protection of Children from Sexual Offences Act, 2012.

Judicial Decisions

9. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
10. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
11. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
12. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
13. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
14. State of Tamil Nadu v. Suhas Katti, 2004 (case concerning online harassment under the Information Technology Act).

Books

15. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publishing.
16. Karnika Seth, Computers, Internet and New Technology Laws, LexisNexis.
17. S. K. Verma and Raman Mittal (eds.), Legal Dimensions of Cyber Space, Indian Law Institute.
18. Pavan Duggal, Cyber Law: The Indian Perspective.

Government Reports and Official Publications

19. Ministry of Electronics and Information Technology, Government of India, publications concerning cybersecurity and information technology.
20. Indian Computer Emergency Response Team (CERT-In), Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents, 28 April 2022.
21. Ministry of Home Affairs, Government of India, publications concerning the Indian Cyber Crime Coordination Centre (I4C).
22. National Crime Records Bureau, Crime in India reports.
23. Government of India, National Cyber Crime Reporting Portal, https://cybercrime.gov.in.

International Materials

24. Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.
25. United Nations, United Nations Convention against Transnational Organized Crime, 2000.
26. United Nations Office on Drugs and Crime (UNODC), publications on cybercrime and international cooperation.
27. Council of Europe, publications concerning electronic evidence and international cooperation in cybercrime investigations.