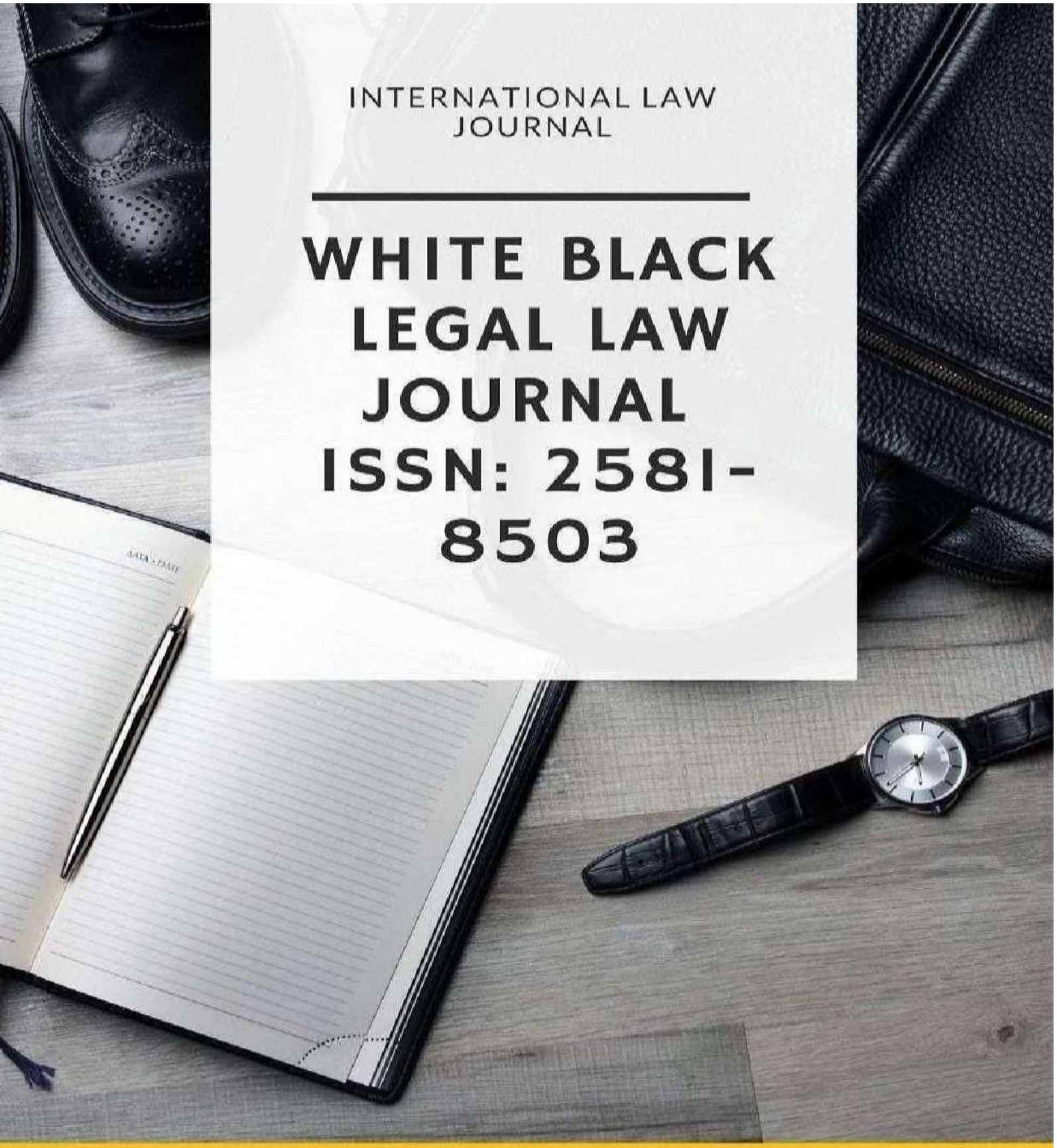

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DIGITAL CRIME AND FORENSIC SCIENCE IN INDIAN

AUTHORED BY - MONISHA S & MRS. A BHUVANESHWARI

ABSTRACT

Digital crime has emerged as one of the most pressing challenges for the Indian criminal justice system, demanding a response that combines legal reform with scientific investigation. This dissertation examines digital crime and forensic science in India through doctrinal legal research, analysing the substantive provisions of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Digital Personal Data Protection Act, 2023, alongside the principles of digital forensic practice such as chain of custody, hashing and authentication. The study evaluates landmark judicial decisions including *Anvar P.V.*, *Arjun Panditrao*, *Puttaswamy* and *Shreya Singhal*, and undertakes comparative analysis with the United States, United Kingdom, European Union and Singapore. It further assesses emerging challenges posed by artificial intelligence, deepfakes, cryptocurrency, the Internet of Things and cloud computing. The research concludes that effective control of digital crime requires not only updated legislation but also forensic capacity, judicial training, institutional coordination and rights-respecting investigative procedures.

CHAPTER I

INTRODUCTION

1.1 Background of the Study

Digital technology has become a central part of social, commercial, educational and governmental life in India. Banking, communication, education, health services, business transactions and public administration are increasingly conducted through electronic platforms. The growth of smartphones, digital payments, cloud storage and social media has produced enormous public benefits, but it has also created a new field of criminal activity. Crimes which were once committed in physical spaces are now planned, executed, concealed and monetised through computers, networks and digital devices.

Digital crime, commonly described as cybercrime, refers to unlawful conduct in which

a computer, computer network, communication device or electronic data is either the object of the offence or the instrument through which the offence is committed. It includes hacking, phishing, identity theft, online financial fraud, ransomware, unauthorised access, cyberstalking, cyber defamation, data theft, child sexual abuse material, cyber terrorism and attacks on critical information infrastructure. The offender may be an individual, an organised criminal group, an insider, a foreign actor or a technically skilled network of anonymous participants.

Unlike conventional crime, digital crime is borderless, fast moving and evidence-sensitive. A fraudulent transaction may be executed in seconds; a malicious file may pass through servers located in multiple jurisdictions; and evidence may disappear if a device is formatted, encrypted or remotely wiped. These features create special problems for police investigation, prosecution and trial. The traditional criminal justice system depends heavily on physical evidence and eyewitness testimony, whereas cybercrime investigation depends on the scientific recovery and authentication of electronic evidence.

Digital forensic science therefore occupies a crucial position in modern criminal justice. It is the scientific process of identifying, collecting, preserving, analysing and presenting data from electronic sources in a legally admissible manner. The discipline includes computer forensics, mobile device forensics, network forensics, cloud forensics, email forensics, memory forensics and malware analysis. It helps investigators trace offenders, reconstruct events, recover deleted files, establish authorship, identify access logs, determine data tampering and connect digital actions to human suspects.

In India, the legal framework for digital crime and electronic evidence has developed through the Information Technology Act, 2000, provisions of the Indian Penal Code, 1860, the Bharatiya Nyaya Sanhita, 2023, the Code of Criminal Procedure, 1973, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023. The Digital Personal Data Protection Act, 2023 has further strengthened the legal discussion around privacy, personal data, consent and misuse of information. The judiciary has also shaped this area through leading decisions on electronic evidence, privacy and intermediary liability.[1]

This dissertation studies digital crime and forensic science in India from a legal perspective. It examines the nature of digital offences, the development of forensic science, the statutory framework, evidentiary rules, judicial interpretation and practical challenges in investigation. The study is especially relevant for legal education because criminal litigation now frequently involves electronic messages, CCTV footage, call detail records, metadata, server logs, screenshots, emails, digital payment records and social media content.

1.2 Meaning and Scope of Digital Crime

Digital crime may be understood broadly as any criminal act involving a computer system, digital network or electronic data. It covers both cyber-dependent offences and cyber-enabled offences. Cyber-dependent offences are those which can exist only because of computer technology, such as hacking, denial-of-service attacks, malware distribution and unauthorised access. Cyber-enabled offences are conventional crimes made easier by digital technology, such as cheating, extortion, stalking, defamation, obscenity, impersonation and financial fraud.

The scope of digital crime is expanding continuously because every new technology generates new opportunities for misuse. Digital payment systems create opportunities for UPI fraud and phishing; cloud computing creates problems of jurisdiction and data control; artificial intelligence creates risks of deepfakes and automated fraud; and social media platforms create opportunities for harassment, misinformation and identity abuse. The law must therefore remain technologically neutral while still providing specific mechanisms for investigation and punishment.

For a law student, the subject is important because digital crime is not merely a technical issue. It involves constitutional rights, privacy, criminal procedure, evidence law, corporate compliance, international cooperation, data protection and human rights. Cybercrime investigation must balance public safety and individual liberty. Excessive surveillance may violate privacy, while weak investigation may allow organised offenders to escape liability.

1.3 Meaning and Importance of Digital Forensic Science

Digital forensic science is the application of scientific methods to electronic evidence. It begins when investigators identify relevant digital sources such as laptops, mobile phones, hard disks, CCTV systems, cloud accounts, routers, servers, email accounts or social media profiles. The evidence must then be collected without alteration, preserved through hashing and documentation, analysed through reliable tools, and presented in court through legally acceptable reports and expert testimony.

The most important feature of digital forensics is preservation of integrity. Electronic evidence is fragile because it can be changed by ordinary use, system updates, malware, remote access or mishandling. Forensic investigators therefore create bit-by-bit images of storage media and calculate hash values such as MD5 or SHA to prove that the copy examined is identical to the original. This process supports the chain of custody and assists the court in determining reliability.[2]

Digital forensics is important not only in cybercrime cases but also in ordinary criminal and civil matters. Murder investigations may involve call records, location data and CCTV footage; matrimonial disputes may involve messages and emails; corruption cases may involve digital payment trails; and commercial disputes may involve electronic contracts and server records. The growth of electronic evidence has made digital forensic knowledge essential for police officers, lawyers, prosecutors and judges.

1.4 Literature Review

Digital crime and forensic science have attracted substantial scholarly attention in India. Pavan Duggal's work on cyber law has provided a foundational analysis of the Information Technology Act, 2000 and related developments, with particular attention to procedural issues, intermediary liability and emerging offences. His writings emphasise that effective cyber law requires constant updating in response to technological change.

Vakul Sharma's commentary on Information Technology Law and Practice offers a section-wise analysis of the IT Act and connects statutory provisions with judicial interpretation. The work has been particularly useful for understanding the relationship between cyber-specific offences under sections 43, 66 and 66C of the IT Act and general criminal law provisions.

Nandan Kamath's study of computers, internet and e-commerce law and Rodney D. Ryder's Guide to Cyber Laws have collectively examined civil and criminal aspects of cyber regulation, contractual issues in electronic commerce and emerging questions of digital governance.

On the forensic side, B.R. Sharma's work on forensic science in criminal investigation provides foundational material on the scientific basis of evidence collection and analysis. While his focus is broader than digital forensics, the principles of preservation, chain of custody and authentication apply equally to electronic evidence.

Reports of the National Crime Records Bureau, the Indian Computer Emergency Response Team (CERT-In) and the Ministry of Electronics and Information Technology document patterns of cybercrime, statistical trends and policy initiatives. These materials are essential for understanding the scale of the problem and the institutional response.

However, there is comparatively limited integrated legal scholarship that brings together substantive cyber offences, forensic procedure, evidentiary requirements and judicial interpretation in a single analytical framework. Most existing studies focus either on technical security or on statutory provisions in isolation. This dissertation seeks to bridge that gap.

1.5 Significance of the Study

This study is significant because India is undergoing rapid digitalisation. Government services, banking, education, health care and commerce are being digitised at a large scale. As citizens become increasingly dependent on digital systems, the risk of misuse also increases. Cybercriminals exploit lack of awareness, weak security practices and delays in reporting. Many victims are ordinary citizens, senior citizens, students, small businesses and women using social media platforms.

The study is also significant from the perspective of criminal justice. Investigation agencies often face difficulty in tracing offenders, obtaining data from service providers, preserving volatile evidence and explaining technical findings in court. Without proper forensic procedure, electronic evidence may be rejected or given little evidentiary value. This creates a gap between the commission of digital crimes and successful conviction.

From a legal perspective, the study analyses whether Indian law is adequate to address digital crime and whether forensic science is being effectively integrated into investigation and adjudication. It also examines the need for capacity building, specialised cybercrime courts, standard operating procedures, training of police officials and better cooperation between forensic laboratories and courts.

1.6 Aim and Objectives of the Study

Aim

The primary aim of this research is to analyse the legal and forensic framework governing digital crime in India and to evaluate the role of digital forensic science in investigation, prosecution and adjudication of cyber offences.

Objectives

1. To study the concept, evolution and forms of digital crime in India.
2. To examine the development and principles of digital forensic science.
3. To analyse the statutory framework governing cybercrime, electronic evidence and data protection in India.
4. To evaluate the role of courts in interpreting electronic evidence and digital rights.
5. To identify major investigative, legal, technical and institutional challenges.
6. To suggest reforms for strengthening cybercrime investigation and forensic capacity in India.

1.7 Research Problem

The central research problem is that digital crime is increasing rapidly while the criminal justice system often lacks sufficient technical capacity, forensic infrastructure and procedural uniformity to investigate and prosecute such offences effectively. Although India has enacted laws relating to cybercrime and electronic evidence, enforcement remains uneven. The gap between legal provisions and forensic practice affects victim protection, prosecution success and public confidence in the justice system.

1.8 Research Questions

This research seeks to answer the following questions:

7. What are the major forms and characteristics of digital crime in India?
8. How does digital forensic science assist in the detection and prosecution of cyber offences?
9. Whether the existing Indian legal framework adequately addresses digital crime and electronic evidence?
10. What challenges arise in collection, preservation and admissibility of electronic evidence?
11. How has the Indian judiciary contributed to the development of cyber law and digital evidence jurisprudence?
12. What legal, institutional and technological reforms are required?

1.9 Hypothesis

The study proceeds on the hypothesis that the effective control of digital crime in India depends not merely on the existence of cyber laws, but on the proper integration of digital forensic science, trained investigators, reliable evidence handling, judicial understanding of technology and strong institutional coordination.

1.10 Research Methodology

This research adopts a doctrinal method of legal research. The study relies on primary sources such as statutes, rules, judicial decisions, government notifications and official guidelines. It also relies on secondary sources such as books, journal articles, reports, commentaries and online legal materials. The research is analytical and descriptive in nature and focuses on the legal and forensic dimensions of digital crime in India. No empirical field survey has been conducted.

1.11 Research Gap

Existing literature on cybercrime often focuses either on technical security or on statutory provisions. There is comparatively less integrated legal research that connects cyber offences, forensic investigation, electronic evidence and judicial standards in a single framework. This study attempts to bridge that gap by examining digital crime and forensic science together as interdependent parts of the criminal justice process.

1.12 Limitations of the Study

The study is limited to the Indian legal system and focuses primarily on criminal law, evidence law and forensic aspects. It does not include laboratory experimentation or empirical interviews with forensic experts. The technological discussion is limited to concepts necessary for legal analysis. Comparative references are used only where they help evaluate Indian law and practice.

1.13 Scheme of the Study

The dissertation is divided into seven chapters. Chapter I introduces the topic, research problem, objectives, methodology and scope. Chapter II discusses the historical and theoretical framework of digital crime and forensic science. Chapter III analyses the legislative framework in India. Chapter IV examines issues and challenges in investigation, evidence handling and enforcement. Chapter V studies the role of the judiciary. Chapter VI provides a comparative analysis of digital crime and forensic laws with other countries. Chapter VII presents findings, conclusion and suggestions for reform.

Footnotes

1. Information Technology Act, 2000, Preamble and Statement of Objects and Reasons.
2. Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
3. Bharatiya Sakshya Adhiniyam, 2023, ss. 61-63.
4. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
5. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

CHAPTER II

HISTORICAL AND THEORETICAL FRAMEWORK

2.1 Introduction

The development of digital crime and forensic science must be understood within the wider history of technological change. Every major communication technology has produced corresponding forms of misuse. Postal systems were used for fraud, telephones for impersonation, banking systems for financial deception, and computers for unauthorised access and data theft. The internet intensified these problems by allowing offenders to operate anonymously and across borders.

Digital crime is not a completely new category of wrongdoing. Many cyber offences are digital versions of traditional crimes such as cheating, forgery, extortion and defamation. However, the method, speed, scale and evidentiary nature of such crimes are new. A single phishing campaign can affect thousands of victims. A ransomware attack can paralyse hospitals, companies or public institutions. A deepfake can damage reputation within minutes. These features justify a specialised legal and forensic response.

2.2 Evolution of Cybercrime

In the early stages of computerisation, cybercrime was largely associated with unauthorised access and experimentation by technically skilled individuals. As personal computers and networks became common, offences expanded to include software piracy, password theft, virus distribution and data manipulation. With the growth of internet banking and e-commerce, financial cybercrime became a major concern. Later, smartphones and social media created new forms of harassment, stalking, identity theft and misinformation.

In India, cybercrime became a legal concern with the spread of internet services in the late 1990s and early 2000s. The Information Technology Act, 2000 was enacted to give legal recognition to electronic records and digital signatures and to address certain computer-related offences. The 2008 amendment expanded the penal provisions and introduced offences relating to identity theft, cheating by personation using computer resources, violation of privacy and cyber terrorism.[1]

Today, cybercrime has become organised and commercial. Offenders use fake call centres, mule bank accounts, cryptocurrency, social engineering, malware kits, SIM swapping and anonymising tools. The victim may not know the offender, the place of commission may be distributed, and the evidence may exist in multiple digital locations. This evolution demands

updated legal interpretation and stronger forensic capacity.

2.3 Evolution of Digital Forensic Science

Digital forensics emerged from the need to examine computers in a scientifically reliable manner. Initially, investigators simply searched devices for relevant files. As storage systems became more complex, forensic science developed systematic methods for imaging disks, recovering deleted data, analysing file systems, extracting metadata and maintaining audit trails. Modern digital forensics now includes mobile applications, encrypted devices, cloud accounts, network packets, malware, blockchain transactions and Internet of Things devices.

The discipline rests on the idea that digital actions leave traces. A user opening a file, sending an email, installing software, connecting a USB device or logging into a server may leave timestamps, logs, registry entries, cache files or metadata. These traces can help reconstruct events. However, unlike physical traces, digital traces are easily altered. Therefore, forensic procedure must ensure that evidence remains authentic and reliable.

The forensic process usually involves identification, preservation, acquisition, examination, analysis and presentation. Identification means locating relevant devices and accounts. Preservation means preventing alteration. Acquisition means creating forensic copies. Examination and analysis involve extracting and interpreting data. Presentation means explaining the findings in a report and, when necessary, through expert testimony in court.

2.4 Theoretical Principles of Digital Forensics

The first theoretical principle is the digital adaptation of Locard's Exchange Principle. In physical forensics, every contact leaves a trace. In digital environments, every interaction with a computer system may leave some form of data trace, such as logs, cookies, IP addresses, metadata, temporary files or access records. The challenge is to locate, preserve and interpret those traces accurately.

The second principle is chain of custody. Chain of custody is the documented history of evidence from the time it is collected until it is produced in court. In digital cases, it includes details of seizure, imaging, hash values, storage, transfer, examination and reporting. If chain of custody is broken, the defence may argue that the evidence was altered or substituted.

The third principle is integrity through hashing. A hash value is a unique digital fingerprint of data. If even one bit changes, the hash value changes. Investigators therefore calculate hash values for original devices and forensic images to demonstrate that the evidence

examined is unchanged. Courts rely on such methods to assess authenticity.

The fourth principle is repeatability and reliability. Forensic findings should be capable of being verified by another competent examiner using accepted methods. Tools used for extraction and analysis should be validated wherever possible. The expert should explain both findings and limitations in clear language.

2.5 Electronic Evidence and Legal Theory

Electronic evidence differs from oral and physical evidence. It may be intangible, machine-generated, automatically stored and dependent on technical systems. A CCTV recording, for example, is not testimony by a person but a digital record created by a device. A server log may be automatically generated by software. The law must therefore create rules for proving authenticity, reliability and relevance.

Indian evidence law has responded by recognising electronic records and prescribing certification requirements. Section 65B of the Indian Evidence Act, 1872 became central to the admissibility of electronic records. The Bharatiya Sakshya Adhiniyam, 2023 continues the recognition of electronic or digital records and contains provisions for admissibility. These provisions reflect the idea that courts need assurance that electronic evidence was produced by a reliable system and was not tampered with.[3]

At the theoretical level, electronic evidence raises questions of authorship and attribution. A message from a phone does not automatically prove that the owner typed it. A login from an IP address does not conclusively identify a person. Forensic analysis must therefore connect devices, accounts, behaviour, timestamps and surrounding circumstances to establish attribution.

2.6 Constitutional Dimensions

Digital crime investigation often requires access to personal devices, communications and data. This creates a tension between investigation and privacy. The Supreme Court in K.S. Puttaswamy v. Union of India recognised privacy as a fundamental right under Article 21. Any invasion of privacy must satisfy legality, necessity and proportionality. Therefore, cybercrime investigation must be lawful, targeted and subject to procedural safeguards.[2]

At the same time, the State has a duty to protect citizens from fraud, harassment, exploitation and cyber attacks. A balanced legal framework must allow effective investigation while preventing arbitrary surveillance and misuse of power. Digital forensic science assists this balance because it encourages evidence-based investigation rather than speculative or

intrusive methods.

2.7 Conclusion

The historical and theoretical framework shows that digital crime is a product of technological development and that digital forensic science is essential to modern criminal justice. The principles of trace evidence, chain of custody, hashing, reliability, authenticity and privacy form the foundation for understanding the legislative framework discussed in the next chapter.

Footnotes

1. Information Technology Act, 2000, ss. 43, 66, 66C, 66D and 66F.
2. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
3. Indian Evidence Act, 1872, s. 65B.
4. Bharatiya Sakshya Adhiniyam, 2023, ss. 61-63.
5. State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.

CHAPTER III
LEGISLATIVE FRAMEWORK AND ANALYSIS OF EXISTING LAWS

3.1 Introduction

India has a multi-layered legal framework for digital crime and forensic evidence. No single statute deals with every aspect of cybercrime. The Information Technology Act, 2000 provides the core cyber law framework. The Indian Penal Code, 1860 and the Bharatiya Nyaya Sanhita, 2023 deal with traditional offences committed through digital means. Evidence law governs admissibility of electronic records. Criminal procedure governs search, seizure, arrest and investigation. Data protection law regulates personal data. Sectoral regulations and CERT-In directions impose cybersecurity obligations.

This chapter analyses the main legal provisions relevant to digital crime and forensic science in India. The discussion focuses on how the law criminalises digital conduct, regulates electronic evidence and supports investigation.

3.2 Information Technology Act, 2000

The Information Technology Act, 2000 was enacted to provide legal recognition to electronic records and electronic commerce. It also contains civil and criminal provisions dealing with computer-related misconduct. The Act recognises electronic records and digital

signatures, thereby enabling electronic governance and electronic transactions. Its penal provisions were strengthened by the Information Technology (Amendment) Act, 2008.[1]

Section 43 provides for compensation for unauthorised access, downloading, copying, extraction of data, introduction of computer contaminant or virus, disruption of computer systems and denial of access. Section 66 criminalises computer-related offences when acts under section 43 are committed dishonestly or fraudulently. Section 66C punishes identity theft, including fraudulent use of electronic signatures, passwords or unique identification features. Section 66D punishes cheating by personation using computer resources, which is commonly invoked in phishing and online fraud cases.

Section 66E deals with violation of privacy by capturing, publishing or transmitting images of private areas without consent. Section 66F deals with cyber terrorism. Sections 67, 67A and 67B deal with publishing or transmitting obscene, sexually explicit and child sexual abuse material in electronic form. Section 69 empowers interception, monitoring or decryption subject to statutory conditions. Section 70 protects critical information infrastructure, while section 70B establishes CERT-In as the national nodal agency for cyber incident response.

The IT Act is significant because it recognises both the civil and criminal consequences of misuse of computer resources. However, its effectiveness depends on timely reporting, technical investigation, cooperation of intermediaries and forensic proof. Many offences under the Act require proof of dishonest or fraudulent intention, unauthorised access, transmission, publication or identity misuse. Digital forensic evidence therefore becomes essential to connect the actus reus and mens rea.

3.3 Indian Penal Code, 1860 and Bharatiya Nyaya Sanhita, 2023

Many cyber offences are prosecuted under general criminal law because the underlying wrong remains cheating, forgery, extortion, intimidation, stalking, defamation or criminal breach of trust. For example, online financial fraud may involve cheating; fake job portals may involve deception; misuse of digital documents may involve forgery; and threats through messaging platforms may involve criminal intimidation.

Historically, provisions of the Indian Penal Code such as sections 419, 420, 463, 465, 468, 471, 499, 500, 503, 506, 354D and 509 were relevant to cyber-enabled offences. With the introduction of the Bharatiya Nyaya Sanhita, 2023, criminal law has been reorganised while retaining many substantive concepts. Legal analysis of digital crime must therefore consider both cyber-specific provisions and general penal provisions applicable to conduct committed through electronic means.

The advantage of using general penal law is flexibility. The disadvantage is that traditional provisions may not fully capture the technical nature of cyber offences. Therefore, investigators and prosecutors often combine provisions of the IT Act with provisions of general criminal law.

3.4 Evidence Law: Indian Evidence Act and Bharatiya Sakshya Adhiniyam

Electronic evidence is central to digital crime cases. The Indian Evidence Act, 1872 recognised electronic records and section 65B laid down the special procedure for proving electronic records. The Supreme Court in Anvar P.V. v. P.K. Basheer held that electronic records must satisfy section 65B for admissibility when produced as secondary evidence.[4] Later, in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, the Court clarified the mandatory nature of the certificate and addressed situations where the party does not control the device.[5]

The Bharatiya Sakshya Adhiniyam, 2023 modernises evidence law and recognises electronic or digital records. Sections 61 to 63 are particularly important. They deal with electronic or digital records, special provisions relating to such records and their admissibility. The law reflects the need to treat electronic records as documentary evidence while maintaining safeguards for authenticity.[3]

The certificate requirement serves an evidentiary function. It states the manner of production, identifies the device, confirms regular use and reliability, and certifies that the record was produced by a computer during ordinary activities. In forensic practice, this requirement works alongside hash values, seizure memos, imaging reports and expert opinions.

3.5 Criminal Procedure and Search of Digital Devices

Cybercrime investigation often requires seizure of computers, mobile phones, storage devices, CCTV systems and servers. Criminal procedure law governs search, seizure, arrest, investigation and production of evidence. Investigators must follow lawful procedure because illegally or improperly collected evidence may be challenged in court and may also violate privacy rights.

When digital devices are seized, investigators should document the condition of the device, prevent remote access, avoid unnecessary use of the device, create forensic images and maintain chain of custody. In mobile phone cases, the device may be placed in airplane mode or a Faraday bag to prevent remote wiping. In cloud cases, investigators may need lawful requests to service providers. These procedural steps are not merely technical; they protect the

evidentiary value of the material.

3.6 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 provides a framework for processing digital personal data in a manner that recognises both individual data protection and lawful processing. Although it is not a cybercrime statute in the narrow sense, it is relevant because many digital crimes involve misuse of personal data, identity theft, unauthorised sharing and profiling. The Act strengthens the legal environment around consent, duties of data fiduciaries and protection of personal information.[2]

Personal data protection is closely connected to cybercrime prevention. Poor data security can lead to data breaches, phishing, identity fraud and financial crime. Organisations handling personal data must adopt responsible practices. A stronger data protection regime can reduce opportunities for digital crime and support accountability after breaches.

3.7 CERT-In Directions and Cybersecurity Governance

CERT-In functions as the national nodal agency for cyber incident response under section 70B of the IT Act. The 2022 CERT-In Directions require specified entities to report certain cyber incidents within prescribed time and maintain relevant logs. These directions are important for forensic investigation because timely reporting and log preservation help investigators trace attacks, identify compromised systems and reconstruct events.[6]

Log retention is particularly significant. In many cybercrime cases, the most important evidence consists of IP logs, access logs, transaction logs, email headers and server activity records. If such logs are not preserved, attribution becomes difficult. Cybersecurity governance therefore supports criminal investigation by ensuring that digital traces remain available.

3.8 Intermediary Liability and Platform Regulation

Intermediaries such as social media platforms, hosting services, search engines and messaging platforms play an important role in digital crime cases. They may possess user data, logs, content records and account details necessary for investigation. Indian law provides safe harbour protection to intermediaries subject to due diligence obligations. Courts have recognised that intermediary liability must be balanced with free speech, innovation and accountability.

Platform regulation is especially relevant in cases involving online abuse, obscene content, impersonation, fake profiles, hate speech, cyber defamation and financial scams.

Quick grievance redressal, traceability subject to law, preservation requests and cooperation with lawful investigations are important components of digital governance.

3.9 Analysis of Legislative Framework

India has a substantial legal framework for digital crime. The IT Act provides cyber-specific offences. General criminal law covers deception, forgery, extortion and harassment. Evidence law governs admissibility. Data protection law addresses personal data misuse. CERT-In directions support incident reporting. However, fragmentation remains a challenge. Investigators must navigate multiple statutes and technical procedures.

The main weakness is not absence of law but uneven implementation. Cyber police stations require trained personnel, forensic laboratories require capacity, prosecutors require technical literacy and courts require reliable expert assistance. Legal reforms must therefore focus on institutional strengthening as much as statutory drafting.

3.10 Conclusion

The legislative framework in India provides a foundation for dealing with digital crime and electronic evidence. Nevertheless, effective enforcement depends on forensic capability, procedural compliance and inter-agency coordination. The next chapter examines the practical issues and challenges arising in investigation and prosecution.

Footnotes

1. Information Technology Act, 2000, ss. 43, 66, 66C, 66D, 66E, 66F, 67, 69, 70 and 70B.
2. Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
3. Bharatiya Sakshya Adhiniyam, 2023, ss. 61-63.
4. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
5. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
6. CERT-In Directions dated 28 April 2022 issued under s. 70B(6) of the IT Act.

CHAPTER IV

ISSUES, CHALLENGES AND ANALYSIS OF THE SUBJECT MATTER

4.1 Introduction

Digital crime creates legal, technical and institutional challenges that differ from ordinary criminal investigation. The offender may be unknown, the evidence may be volatile, the victim may be in one State while the server is in another country, and the proceeds may be transferred through digital wallets, bank accounts or cryptocurrency. Investigation must therefore be fast, technically competent and legally sound.

This chapter analyses major forms of cybercrime in India and the challenges faced in forensic investigation and prosecution.

4.2 Online Financial Fraud

Online financial fraud is one of the most common forms of digital crime. It includes phishing, vishing, UPI fraud, fake customer care numbers, fake investment schemes, loan app frauds, SIM swapping, OTP theft, QR code fraud and mule account networks. The offender deceives the victim into disclosing credentials or authorising a transaction. The money may be transferred quickly through multiple accounts, making recovery difficult.

Forensic investigation in such cases involves transaction tracing, call detail records, bank account analysis, device examination, IP logs, messaging records and beneficiary identification. The challenge is speed. If freezing instructions are delayed, funds may be withdrawn or layered through multiple accounts. Coordination among police, banks, payment intermediaries and cybercrime portals is therefore crucial.

4.3 Hacking, Malware and Ransomware

Hacking involves unauthorised access to computer systems. It may be done for data theft, disruption, espionage, revenge or financial gain. Malware is malicious software designed to damage, control or extract information from systems. Ransomware encrypts data and demands payment for restoration. Such attacks can affect individuals, companies, hospitals, educational institutions and government agencies.[1]

Forensic analysis of malware requires specialised expertise. Investigators may examine malicious files, system logs, registry entries, network traffic, command-and-control connections and encryption artefacts. In ransomware cases, attribution is difficult because attackers use anonymity networks, foreign servers and cryptocurrency. Nevertheless, forensic

evidence can identify entry points, affected systems and indicators of compromise.

4.4 Cyberstalking, Online Harassment and Gendered Cybercrime

Digital platforms have created new forms of harassment. Cyberstalking, morphing, non-consensual sharing of intimate images, fake profiles, doxxing, threats, obscene messages and reputation attacks disproportionately affect women and vulnerable groups. These offences cause psychological harm, social stigma and fear. Victims may hesitate to report due to embarrassment or lack of trust.

Forensic investigation requires preservation of screenshots, URLs, profile details, message metadata, platform reports and device data. However, screenshots alone may not be sufficient unless properly authenticated. Investigators must act quickly because offending content may be deleted. Platform cooperation is essential to identify account creation details, IP logs and linked identifiers.

4.5 Child Sexual Abuse Material and Obscene Content

The circulation of child sexual abuse material and obscene electronic content is a serious digital crime. The IT Act contains provisions relating to obscene, sexually explicit and child sexual abuse material. Investigation requires careful handling because evidence itself is illegal and sensitive. Forensic laboratories must follow strict protocols to avoid unnecessary copying and exposure.

International cooperation is often required because such material may be hosted on foreign servers. Hash-based detection, content takedown procedures, platform reporting and specialised victim protection mechanisms are necessary. Courts must balance evidentiary requirements with dignity and privacy of victims.

4.6 Challenges in Collection and Preservation of Evidence

The first major challenge is volatility. Digital evidence can be deleted, overwritten, encrypted or remotely wiped. Live data such as RAM contents and network connections may disappear when a device is powered off. Investigators must decide whether to conduct live acquisition or shut down a device. This decision requires training and standard operating procedures.

The second challenge is authenticity. Courts must be satisfied that the electronic record produced is genuine. Improper collection, absence of hash values, missing chain of custody or lack of certification may weaken the prosecution case. Digital evidence should therefore be

handled by trained personnel or under their supervision.[2]

The third challenge is volume. A single mobile phone may contain thousands of messages, images, app records and location data. Investigators must identify legally relevant material without violating privacy unnecessarily. Forensic tools help filter data, but human legal judgment remains essential.

4.7 Encryption, Anonymity and Attribution

Encryption protects privacy and cybersecurity, but it can also complicate investigation. Devices, messaging applications and cloud services may be encrypted. Offenders may use VPNs, proxy servers, Tor networks and fake accounts. As a result, attribution becomes one of the hardest parts of digital investigation.

Attribution requires correlation of multiple sources: device possession, login patterns, recovery emails, phone numbers, payment trails, IP addresses, location data, witness evidence and conduct before and after the offence. A single technical indicator may be insufficient. The prosecution must present a coherent chain of circumstances connecting the accused with the digital act.

4.8 Jurisdictional and Cross-Border Problems

Digital crimes often cross territorial boundaries. A victim may be in Tamil Nadu, the suspect may be in another State, the platform may be owned by a foreign company and the server may be outside India. This creates problems of jurisdiction, evidence access and delay. Mutual legal assistance processes may take time, while electronic evidence may be retained only for limited periods.

Cross-border cooperation is essential for serious cybercrime, especially ransomware, child exploitation, financial fraud and cyber terrorism. India must strengthen international cooperation, standardise preservation requests and build faster mechanisms for obtaining lawful access to data.

4.9 Capacity and Infrastructure Challenges

Many police stations lack specialised cyber training and forensic equipment. Even where cyber cells exist, the volume of complaints may be far greater than available personnel. Forensic science laboratories may face backlogs. Delays in examination may affect trial timelines and victim confidence. There is also a shortage of prosecutors and judges with adequate technical understanding.[3]

Capacity building must include regular training for police, prosecutors, judicial officers and forensic experts. Law schools should also include cyber law and electronic evidence as practical subjects. Public awareness is equally important because many cybercrimes succeed through social engineering rather than technical hacking.

4.10 Admissibility and Courtroom Presentation

Even when digital evidence is collected, it must be presented in court in an understandable and legally admissible manner. Technical reports should explain the device examined, method of acquisition, tools used, hash values, findings and limitations. The expert must avoid excessive jargon and should be prepared for cross-examination.

Lawyers must understand the difference between original devices, forensic images, screenshots, metadata, logs and certificates. Courts should insist on reliability but should also avoid unrealistic technical expectations. The purpose of evidence law is to ensure authenticity and fairness, not to exclude reliable evidence on purely mechanical grounds.

4.11 Analysis

The issues discussed above show that digital crime is both a legal and technological problem. The law provides offences and procedures, but successful enforcement depends on technical competence. The main challenge is converting digital traces into legally admissible proof. This requires coordination among investigators, banks, platforms, forensic laboratories, prosecutors and courts.

Another important point is victim protection. Many victims lose money, reputation, privacy and mental peace. The justice system should provide quick reporting channels, freezing of fraudulent transactions, content takedown, counselling support and timely updates. Cybercrime enforcement should not be limited to punishment after trial; it should also include prevention and harm reduction.

4.12 Conclusion

Digital crime investigation in India faces challenges of speed, technology, jurisdiction, capacity and evidence law. Strengthening digital forensic science is essential for overcoming these challenges. The next chapter examines the role of the judiciary in shaping this field.

Footnotes

1. Information Technology Act, 2000, ss. 66C, 66D, 66E, 66F, 67, 67A and 67B.

2. Indian Evidence Act, 1872, s. 65B; Bharatiya Sakshya Adhiniyam, 2023, s. 63.
3. CERT-In Directions dated 28 April 2022.
4. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
5. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

CHAPTER V

ROLE OF JUDICIARY IN THE SUBJECT MATTER

5.1 Introduction

The judiciary has played a major role in developing Indian cyber law and electronic evidence jurisprudence. Courts have interpreted the admissibility of electronic records, recognised privacy as a fundamental right, examined intermediary liability and protected freedom of speech in digital spaces. Judicial decisions are particularly important because technology often changes faster than legislation.

This chapter analyses leading decisions relevant to digital crime and forensic science in India.

5.2 Electronic Evidence and Section 65B

The most important line of cases concerns admissibility of electronic evidence. In State (NCT of Delhi) v. Navjot Sandhu, the Supreme Court had taken a flexible approach to electronic records.[1] However, in Anvar P.V. v. P.K. Basheer, the Court held that section 65B of the Indian Evidence Act is a complete code for admissibility of electronic records and that the certificate requirement is mandatory when electronic evidence is produced as secondary evidence.[2]

The Anvar ruling strengthened evidentiary discipline. It made clear that electronic records cannot be casually produced without satisfying statutory safeguards. This is important in forensic science because authenticity is central to digital proof. The ruling encourages proper certification, preservation and documentation.

In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, the Supreme Court clarified the law further.[3] The Court reaffirmed the mandatory nature of section 65B but recognised practical difficulties where the party does not possess the device. It held that courts may order production of the certificate from the person controlling the device. This decision balances strict evidentiary safeguards with practical access to justice.

5.3 Privacy and Digital Investigation

In K.S. Puttaswamy v. Union of India, the Supreme Court recognised privacy as a fundamental right under Article 21 of the Constitution.[4] The judgment has deep implications for cybercrime investigation. Search of mobile phones, interception of communication, access to cloud accounts and collection of personal data must be supported by law and must satisfy

constitutional standards.

The decision does not prevent investigation; rather, it requires lawful and proportionate investigation. Digital forensic searches should be relevant to the offence and should avoid unnecessary invasion of unrelated personal material. This is especially important because a smartphone contains intimate details of a person's life, including communications, photographs, location history, financial data and personal documents.

5.4 Freedom of Speech and Online Expression

Shreya Singhal v. Union of India is a landmark case in Indian cyber law. The Supreme Court struck down section 66A of the IT Act as unconstitutional for being vague and overbroad.[5] The decision protected freedom of speech under Article 19(1)(a) and held that restrictions on online speech must satisfy constitutional requirements.

This case is significant because cyber law must not become a tool for suppressing lawful expression. At the same time, the Court distinguished between discussion, advocacy and incitement. The judgment shows that digital regulation must balance free speech with legitimate concerns such as public order, defamation, harassment and national security.

5.5 Video Conferencing and Technology in Courts

In State of Maharashtra v. Dr. Praful B. Desai, the Supreme Court recognised the validity of recording evidence through video conferencing.[6] Though not a cybercrime case in the narrow sense, the decision demonstrates judicial acceptance of technology in legal procedure. It also reflects a broader willingness to adapt legal processes to technological realities.

Digital courts, e-filing, virtual hearings and electronic records are now part of the justice system. This development reinforces the importance of understanding digital evidence and forensic reliability.

5.6 CCTV, Digital Records and Adverse Inference

In Tomaso Bruno v. State of Uttar Pradesh, the Supreme Court emphasised the relevance of CCTV footage and modern scientific evidence.[7] The Court observed that non-production of relevant electronic evidence may permit adverse inference in appropriate circumstances. This case indicates that electronic evidence is not merely supplementary; in many cases it may be the best available evidence.

Courts increasingly expect investigating agencies to collect available digital evidence

such as CCTV footage, call records and electronic communications. Failure to do so may weaken the prosecution case.

5.7 Intermediary Liability

In Google India Pvt. Ltd. v. Visakha Industries, the Supreme Court considered issues relating to intermediary liability and online content.[8] The case highlights the complexity of assigning responsibility in digital environments where content may be created by users but hosted or indexed by platforms. Intermediary liability remains an evolving area requiring careful balance between accountability, free speech and technological feasibility.

Courts must ensure that platforms cooperate with lawful investigations while also preserving legitimate safe harbour protection. Overbroad liability may discourage innovation, while complete immunity may harm victims. Judicial interpretation is therefore crucial.

5.8 Judicial Contribution to Forensic Standards

The judiciary contributes to forensic standards by insisting on authenticity, certification and reliability. When courts require proper chain of custody and section 65B compliance, they indirectly improve investigation practices. Forensic science gains legal value only when courts understand and accept its methods.

At the same time, courts face challenges in dealing with highly technical evidence. Judges may require assistance from expert witnesses, forensic reports and clear presentation by counsel. Judicial training in cyber law and electronic evidence is therefore necessary.

5.9 Limitations of Judicial Intervention

Judicial decisions can clarify law, but courts cannot alone solve the problem of cybercrime. Effective enforcement requires trained investigators, forensic laboratories, updated tools, cooperation from intermediaries and awareness among citizens. Excessive dependence on courts after harm occurs is insufficient. Preventive governance and institutional reform are equally important.

There is also a need to avoid inconsistent application of electronic evidence rules. Trial courts must receive practical guidance on certificates, hash values, screenshots, CCTV footage, mobile extractions and expert reports. Uniform practice will improve predictability and fairness.

5.10 Conclusion

The Indian judiciary has played a transformative role in recognising digital rights and shaping electronic evidence law. Cases such as Anvar, Arjun Panditrao, Puttaswamy and Shreya Singhal provide the legal foundation for digital crime adjudication. The next chapter undertakes a comparative analysis with the cybercrime and digital forensic frameworks of other countries.

Footnotes

1. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
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. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
5. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
6. State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
7. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
8. Google India Pvt. Ltd. v. Visakha Industries, (2020) 4 SCC 162.

CHAPTER VI

COMPARATIVE ANALYSIS OF LAWS WITH OTHER COUNTRIES

6.1 Introduction

Comparative legal analysis plays an important role in understanding how different jurisdictions address similar challenges. Digital crime is a global phenomenon. Offences such as hacking, ransomware, online financial fraud, child sexual exploitation, identity theft and data breaches do not respect national boundaries. Many cybercrime investigations require cooperation between authorities of multiple countries, and many evidentiary issues are common across jurisdictions.

By examining how countries such as the United States, the United Kingdom, member States of the European Union and Singapore regulate digital crime and electronic evidence, it becomes possible to identify best practices that may inform Indian law and policy. Comparative study also helps assess whether Indian provisions are broadly aligned with international standards or whether reform is required.

This chapter does not attempt an exhaustive survey. It focuses on selected jurisdictions that possess relatively developed cybercrime legislation, well-established forensic procedures and active judicial engagement with electronic evidence. The discussion concentrates on aspects that are most relevant to Indian conditions: substantive offences, evidentiary rules, investigative powers, data protection, intermediary regulation and international cooperation.

6.2 Importance of Comparative Cyber Law

Comparative cyber law is important for three reasons. First, cyber offences are increasingly transnational. An attacker in one country can target victims and infrastructure in many others. Effective investigation therefore depends on harmonised offences and mutual cooperation. Second, electronic evidence collected abroad must satisfy domestic admissibility rules. Familiarity with foreign procedures improves the quality of cross-border evidence. Third, technological developments such as cloud computing, encryption and artificial intelligence raise the same questions in every jurisdiction. Studying foreign experience can shorten the learning curve for Indian regulators and courts.

Comparative analysis also helps identify weaknesses in domestic law. Countries with stronger enforcement mechanisms, dedicated cybercrime units and structured forensic standards offer useful models for institutional design. At the same time, comparative borrowing must be cautious: legal transplants must respect constitutional context, federal structure and

existing administrative capacity.

6.3 United States

The United States has one of the most developed cyber law systems in the world. The principal substantive statute is the Computer Fraud and Abuse Act, 1986, which criminalises unauthorised access to protected computers, transmission of malicious code, computer-related fraud and trafficking in passwords. The Act has been amended several times to address evolving threats. It applies broadly to both private systems and government networks.[1]

Procedural and evidentiary aspects are governed by the Electronic Communications Privacy Act, 1986, which contains the Stored Communications Act and provisions on wire interception. These statutes regulate access to stored electronic communications, real-time interception and pen register or trap-and-trace devices. They establish different standards depending on the type of data sought, balancing investigative needs with constitutional protections under the Fourth Amendment.

Investigation is supported by specialised agencies such as the Federal Bureau of Investigation Cyber Division, the Secret Service Electronic Crimes Task Forces and the Department of Justice Computer Crime and Intellectual Property Section. These bodies maintain forensic laboratories, training programmes and partnerships with the private sector.

Federal Rules of Evidence, particularly Rules 901 and 902, govern authentication of electronic records. Recent amendments allow self-authentication of certain electronic records produced by qualified persons through certifications resembling those used for business records. Hash values, metadata and chain-of-custody documentation are routinely used to establish authenticity.

Compared to India, the United States places greater emphasis on detailed procedural standards for electronic surveillance, dedicated forensic capacity at federal level and structured cooperation with private intermediaries through subpoena, warrant and preservation request mechanisms.

6.4 United Kingdom

The United Kingdom's principal cyber-specific statute is the Computer Misuse Act, 1990, which criminalises unauthorised access to computer material, unauthorised access with intent to commit further offences, unauthorised acts impairing operation of computers, and the making, supplying or obtaining of articles for use in such offences.[2] The Act has been amended to address denial-of-service attacks and to reflect the seriousness of attacks on critical national

infrastructure.

Investigatory powers are consolidated in the Investigatory Powers Act, 2016, which regulates interception of communications, acquisition of communications data and equipment interference. The Act introduced a system of judicial oversight through Judicial Commissioners and a tribunal mechanism for redress. While criticised by privacy advocates, the Act represents a structured attempt to bring surveillance under the rule of law.

Cybercrime investigation is led by the National Crime Agency, particularly its National Cyber Crime Unit, supported by Regional Organised Crime Units and local police cyber teams. The Crown Prosecution Service has issued specific guidance for prosecuting cyber-dependent and cyber-enabled offences. The United Kingdom is also a party to the Council of Europe Convention on Cybercrime, which provides a framework for substantive offences, procedural powers and international cooperation.

The UK approach is notable for its judicial oversight of investigative powers, well-defined offences focused on unauthorised conduct and integration of forensic capacity into a national policing structure. India can draw on this model when designing oversight mechanisms for surveillance and intermediary cooperation.

6.5 European Union

The European Union has developed an integrated framework that combines criminal law, data protection and cybersecurity governance. Directive 2013/40/EU on attacks against information systems requires member States to criminalise illegal access, illegal system interference, illegal data interference and illegal interception. It also harmonises minimum penalties and supports cross-border cooperation.[3]

On the data protection side, the General Data Protection Regulation, 2016, applicable since 2018, has significantly influenced global data protection norms. It establishes principles of lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and accountability. It grants individuals strong rights over their personal data and imposes mandatory breach notification on controllers. The Regulation also has extraterritorial reach, affecting non-EU entities offering goods or services to individuals in the EU.

Cybersecurity governance is addressed through the NIS2 Directive, which requires member States to ensure that operators of essential services and digital service providers implement risk management measures and report significant incidents. The European Union Agency for Cybersecurity supports policy implementation and incident response across member States.

Many European countries are parties to the Council of Europe Convention on Cybercrime, also known as the Budapest Convention. The Convention is the principal international treaty in this field. It harmonises substantive cyber offences, defines procedural powers such as expedited preservation and disclosure of stored data and establishes a 24/7 network for international cooperation. Although India is not a party, Indian practice reflects similar principles in many areas.

Compared to India, the European Union demonstrates the value of integrating data protection and cybercrime regulation, mandatory breach notification and harmonised cross-border cooperation. The Indian framework, including the Digital Personal Data Protection Act, 2023 and the IT Act, can be strengthened by drawing on these aspects.

6.6 Singapore

Singapore offers a useful comparative model because of its compact regulatory architecture and strong enforcement focus. The Computer Misuse Act, originally enacted in 1993, criminalises unauthorised access, unauthorised modification, unauthorised use or interception of computer services and obstruction of computer operation. It has been amended to address the trade in personal information obtained through cybercrime and to enable extraterritorial application in defined circumstances.[4]

The Cybersecurity Act, 2018 designates critical information infrastructure and imposes duties of risk assessment, incident reporting and audit on responsible owners. The Personal Data Protection Act, 2012 governs the collection, use and disclosure of personal data and includes a mandatory breach notification regime.

Investigation is led by the Cyber Security Agency for cybersecurity incidents and the Singapore Police Force for criminal matters. Forensic capacity is integrated into the Health Sciences Authority and dedicated police units. Singapore's experience demonstrates the value of clear inter-agency division of responsibility and combined civil and criminal mechanisms.

6.7 Comparative Analysis with India

India's legal framework, consisting of the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023 and CERT-In Directions, broadly addresses the same themes as the jurisdictions discussed above. There are, however, several important differences.

First, in matters of substantive law, the IT Act covers most relevant cyber offences but penalties for several offences are comparatively low and definitions in some areas remain

dated. Periodic statutory revision, similar to that adopted in the United States and United Kingdom, would be useful.

Second, in matters of procedure, India lacks a consolidated statute on investigatory powers comparable to the United Kingdom's Investigatory Powers Act. Provisions for interception, monitoring and decryption are scattered across the IT Act, the Telegraph Act and procedural rules. A consolidated framework with structured oversight would improve clarity and accountability.

Third, in matters of evidence, the Indian framework on electronic records under section 65B of the Indian Evidence Act, 1872 and sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023 is broadly aligned with international standards. However, practical implementation is uneven. Standard forms for certification, judicial training and uniform forensic protocols would bring Indian practice closer to that observed in the United States and United Kingdom.

Fourth, in matters of data protection, the Digital Personal Data Protection Act, 2023 marks a significant step forward and shares many features with the General Data Protection Regulation. However, sector-specific guidance, breach notification timelines and enforcement capacity will determine the practical impact of the Act.

Fifth, in matters of international cooperation, India's reliance on bilateral mutual legal assistance treaties is often slow. Joining or aligning with international instruments such as the Budapest Convention, while addressing sovereignty concerns, would improve the speed of cross-border evidence access.

6.8 Lessons for India

Several lessons emerge from comparative study. India can benefit from clearer division of investigative responsibility between national, State and specialised agencies, similar to the United Kingdom and Singapore models. Structured judicial or statutory oversight of surveillance and interception, modelled on the Investigatory Powers Act, would strengthen the rule of law. Mandatory breach notification, building on existing CERT-In Directions and the Digital Personal Data Protection Act, would improve incident response and forensic preservation.

Forensic capacity can be strengthened through accredited laboratories, validated tools and standardised reporting formats, drawing on practices from the United States and the European Union. Judicial training programmes on electronic evidence, similar to those offered to federal judges in the United States, would improve consistency in trial courts.

Finally, faster and more transparent cooperation with intermediaries through clear preservation requests, time-bound disclosure and oversight of access requests would improve both effectiveness and rights protection.

6.9 Conclusion

Comparative analysis demonstrates that effective regulation of digital crime depends on a combination of clear substantive law, well-defined investigative powers, accredited forensic capacity, strong data protection and active international cooperation. India's framework already covers most of these areas, but international experience offers concrete improvements in oversight, capacity, evidentiary standardisation and cross-border procedure.

The next and final chapter draws together the findings of this dissertation and presents conclusions and recommendations for strengthening the Indian framework on digital crime and forensic science.

Footnotes

1. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (United States).
2. Computer Misuse Act, 1990 (United Kingdom).
3. Directive 2013/40/EU on attacks against information systems (European Union).
4. Computer Misuse Act, 1993 (Singapore).
5. Council of Europe Convention on Cybercrime, Budapest, 23 November 2001.

CHAPTER VII

CONCLUSION AND SUGGESTIONS / RECOMMENDATIONS

7.1 Conclusion

Digital crime has become one of the most serious challenges for the Indian legal system. The growth of internet access, digital payments, social media, cloud storage and mobile communication has created new opportunities for economic and social development. At the same time, it has created new opportunities for criminal exploitation. Cybercriminals misuse technology to deceive citizens, steal data, extort money, harass individuals, attack institutions and threaten national security.

This dissertation has examined digital crime and forensic science in India through legal and doctrinal analysis. It shows that digital crime cannot be addressed only through penal provisions. Effective enforcement requires digital forensic science, procedural safeguards, technical training, institutional coordination and judicial understanding. The key issue is the conversion of electronic traces into reliable legal evidence.

India has a significant legal framework consisting of the Information Technology Act, 2000, general criminal law, evidence law, data protection law and cybersecurity directions. The Bharatiya Sakshya Adhiniyam, 2023 continues the recognition of electronic and digital records, while the Digital Personal Data Protection Act, 2023 strengthens the broader framework around personal data. However, implementation challenges remain serious.

The judiciary has contributed substantially by clarifying the law of electronic evidence, recognising privacy and protecting free speech. Decisions such as Anvar, Arjun Panditrao, Puttaswamy and Shreya Singhal are central to the field. Nevertheless, court decisions must be supported by better investigation practices and forensic infrastructure.

Comparative analysis with the United States, the United Kingdom, the European Union and Singapore confirms that India's framework is broadly aligned with international standards, but offers specific improvements in oversight, forensic capacity, data protection enforcement and international cooperation.

7.2 Key Findings

- Digital crime is rapidly increasing in scope and complexity due to dependence on technology.
- Many cyber offences are traditional crimes committed through digital means, while others are purely technology-dependent.

- Digital forensic science is essential for identifying offenders, preserving evidence and proving electronic records in court.
- India has a broad legal framework, but enforcement is weakened by lack of training, infrastructure and coordination.
- Electronic evidence is fragile and must be collected, preserved and presented with strict procedural safeguards.
- Section 65B jurisprudence and the new evidence framework emphasise authenticity and reliability.
- Privacy is a fundamental right and cyber investigation must follow legality, necessity and proportionality.
- Victim protection, quick reporting, transaction freezing and platform cooperation are essential in cybercrime response.
- Comparative experience supports stronger oversight of investigative powers, mandatory breach notification and accredited forensic capacity.

7.3 Suggestions and Recommendations

7.3.1 Strengthening Digital Forensic Infrastructure

Every State should strengthen cyber forensic laboratories with modern hardware, licensed tools, trained examiners and standard operating procedures. District-level access to basic forensic support should be improved so that evidence is not lost due to delay. Laboratories should maintain quality assurance, documentation and tool validation processes.

7.3.2 Training of Police, Prosecutors and Judges

Cybercrime investigation requires continuous training. Police officers should be trained in seizure of devices, preservation of volatile evidence, preparation of seizure memos, use of cybercrime portals and coordination with banks and intermediaries. Prosecutors should be trained to present electronic evidence effectively. Judicial officers should receive training on electronic records, hash values, metadata, certificates and expert testimony.

7.3.3 Uniform Standard Operating Procedures

India should adopt uniform and practical standard operating procedures for digital evidence handling. These should cover device seizure, mobile phone preservation, cloud evidence requests, forensic imaging, hash calculation, chain of custody, report writing and courtroom presentation. Uniform practice will improve reliability and reduce disputes.

7.3.4 Faster Response to Financial Cyber Fraud

Cyber financial fraud requires immediate action. Banks, payment intermediaries and

police should coordinate through real-time mechanisms for freezing suspicious transactions. Victims should be encouraged to report immediately. Standard timelines and accountability mechanisms should be created for responding to cyber fraud complaints.

7.3.5 Strengthening Cooperation with Intermediaries

Social media platforms, telecom companies, banks and hosting providers often possess crucial evidence. Lawful and time-bound cooperation mechanisms should be strengthened. Preservation requests should be simple, fast and documented. At the same time, privacy safeguards must be maintained to prevent excessive or arbitrary data requests.

7.3.6 Public Awareness and Digital Literacy

Many digital crimes succeed because victims are deceived through social engineering. Public awareness programmes should educate citizens about OTP safety, phishing links, fake investment schemes, privacy settings, reporting mechanisms and safe digital practices. Schools and colleges should include basic cyber hygiene education.

7.3.7 Data Protection and Organisational Accountability

Organisations handling personal data should adopt strong cybersecurity practices. Data minimisation, access control, encryption, audit logs and breach response plans reduce the risk of digital crime. The DPDP Act should be implemented in a manner that promotes accountability without creating unnecessary compliance confusion.

7.3.8 Specialised Cybercrime Courts

Specialised cybercrime courts or designated judges may improve trial efficiency in complex cases. Such courts can develop expertise in electronic evidence, expert testimony and technology-related legal issues. Faster adjudication will strengthen deterrence and victim confidence.

7.3.9 International Cooperation

Since cybercrime is often cross-border, India should strengthen mutual legal assistance, information sharing and cooperation with foreign service providers. Faster procedures for preserving electronic evidence located abroad are necessary. International cooperation is especially important in ransomware, child exploitation, cryptocurrency and cyber terrorism cases.

7.3.10 Oversight of Investigative Powers

Drawing from comparative experience, India should consider consolidating provisions on interception, monitoring and decryption, and introducing structured oversight. Independent review of surveillance practices, judicial authorisation where appropriate and transparent reporting can strengthen both effectiveness and rights protection.

7.4 Final Observations

Digital crime is not a temporary problem. It will become more complex with artificial intelligence, deepfakes, cryptocurrency, Internet of Things devices and cloud computing. The law must therefore remain flexible, technology-neutral and rights-respecting. Forensic science must remain scientifically reliable and legally accountable.

The future of criminal justice in India will depend heavily on the ability of legal institutions to understand technology. Lawyers, judges, police officers and forensic experts must work together. A strong digital forensic system will not only improve conviction in cybercrime cases but also protect innocent persons from wrongful accusation by ensuring evidence-based investigation.

Therefore, the fight against digital crime requires a combination of law, science, ethics, institutional capacity and public awareness. Strengthening digital forensic science is essential for achieving justice in the digital era.

BIBLIOGRAPHY

I. CASES

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
3. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
4. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
5. State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
6. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
7. Sonu alias Amar v. State of Haryana, (2017) 8 SCC 570.
8. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
9. Google India Pvt. Ltd. v. Visakha Industries, (2020) 4 SCC 162.
10. People Interactive (India) Pvt. Ltd. v. Vivek Pahwa, 2016 SCC OnLine Bom 7351.

II. STATUTES AND LEGISLATIONS

1. The Constitution of India, 1950.
2. Information Technology Act, 2000.
3. Information Technology (Amendment) Act, 2008.
4. Indian Penal Code, 1860.
5. Bharatiya Nyaya Sanhita, 2023.

6. Code of Criminal Procedure, 1973.
7. Bharatiya Nagarik Suraksha Sanhita, 2023.
8. Indian Evidence Act, 1872.
9. Bharatiya Sakshya Adhiniyam, 2023.
10. Digital Personal Data Protection Act, 2023.

III. BOOKS

1. Duggal, Pavan, Cyber Law: The Indian Perspective.
2. Ryder, Rodney D., Guide to Cyber Laws.
3. Kamath, Nandan, Law Relating to Computers, Internet and E-Commerce.
4. Sharma, Vakul, Information Technology Law and Practice.
5. Sharma, B.R., Forensic Science in Criminal Investigation and Trials.
6. Jain, M.P., Indian Constitutional Law, LexisNexis.

IV. JOURNAL ARTICLES

1. Articles on cyber law and electronic evidence published in leading Indian law journals.
2. Research studies on digital forensic procedure and chain of custody.
3. Articles analysing judicial interpretation of section 65B of the Indian Evidence Act.
4. Studies on intermediary liability and platform regulation in India.
5. Comparative cyber law studies relating to the Budapest Convention.

V. OFFICIAL MATERIALS AND GOVERNMENT REPORTS

1. CERT-In Directions dated 28 April 2022 issued under section 70B(6) of the Information Technology Act, 2000.
2. Ministry of Electronics and Information Technology, Government of India – Materials on cyber law and cybersecurity.
3. India Code official versions of central statutes.
4. National Cyber Crime Reporting Portal materials.
5. National Crime Records Bureau (NCRB) Reports on Crime in India – Cybercrime statistics and trends.

VI. NEWSPAPERS

1. The Hindu – Reports on cybercrime, data breaches and digital fraud.
2. The Indian Express – Articles on cyber law and electronic evidence.

3. The Times of India – Reports on cybercrime investigation and judicial decisions.

VII. WEBSITES

1. Ministry of Electronics and Information Technology – Government of India.
2. Indian Computer Emergency Response Team (CERT-In) Official Website.
3. National Cyber Crime Reporting Portal (cybercrime.gov.in)

ANNEXURES / APPENDICES

ANNEXURE – I

Important Cyber Law Judgments

This annexure refers to landmark judicial decisions relating to electronic evidence, privacy, online speech, video conferencing and intermediary liability. These include Anvar P.V. v. P.K. Basheer, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, K.S. Puttaswamy v. Union of India, Shreya Singhal v. Union of India, State of Maharashtra v. Dr. Praful B. Desai and Google India Pvt. Ltd. v. Visakha Industries.

ANNEXURE – II

Major Cybercrime Provisions

This annexure includes references to major cybercrime provisions in Indian law. Important provisions include sections 43, 66, 66C, 66D, 66E, 66F, 67, 67A, 67B, 69, 70 and 70B of the Information Technology Act, 2000. General criminal law provisions relating to cheating, forgery, criminal intimidation, stalking and defamation may also apply when committed through electronic means.

ANNEXURE – III

Digital Evidence Checklist

- Identify all relevant devices, accounts, storage media and online platforms.
- Document seizure with date, time, place, condition and identifying details.
- Prevent remote access, network alteration and accidental deletion.
- Create forensic image wherever possible and calculate hash values.
- Maintain chain of custody for every transfer and examination.
- Obtain appropriate electronic evidence certificate where required.
- Prepare clear forensic report explaining method, findings and limitations.

ANNEXURE – IV

Suggested Research Keywords

Cybercrime in India; digital forensics; electronic evidence; section 65B; Bharatiya Sakshya Adhiniyam; Information Technology Act; cyber fraud; phishing; ransomware; CERT-In; data protection; right to privacy; intermediary liability; cyberstalking; forensic chain of custody.