INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER FORENSICS: A COMPREHENSIVE LEGAL AND TECHNICAL ANALYSIS - WITH SPECIAL REFERENCE TO INDIAN STATUTORY FRAMEWORK

AUTHORED BY - SABILA IFFATH SHUJATHULLAH

1. ABSTRACT

Cyber forensics also referred to as digital forensics or computer forensics is an interdisciplinary domain that intersects information technology, law enforcement, and jurisprudence. It encompasses the scientific collection, preservation, examination, analysis, and presentation of digital evidence in a manner that is legally admissible before courts of competent jurisdiction. In the twenty-first century, where virtually every dimension of human activity commercial, personal, governmental, and military has migrated to the digital sphere, the significance of cyber forensics as an instrument of justice cannot be overstated.

This research article provides a comprehensive examination of cyber forensics from a legal and technical perspective, with particular emphasis on the Indian statutory framework. The article critically analyses the Information Technology Act, 2000 (as amended in 2008), the Indian Evidence Act, 1872, the Code of Criminal Procedure, 1973, the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023, as they pertain to the admissibility, collection, and evidentiary weight of digital evidence. The article further examines international conventions, comparative jurisdictional approaches, and landmark judicial pronouncements from the Supreme Court of India and various High Courts.

The article also identifies critical lacunae in the existing Indian legal regime governing cyber forensics, proposes legislative and procedural reforms, and situates Indian cyber forensic law within the global discourse on digital evidence and cybercrime investigation. The research employs doctrinal legal methodology supplemented by analytical and comparative approaches.

Keywords: *Cyber Forensics, Digital Evidence, Information Technology Act 2000, Admissibility, Chain of Custody, Cybercrime Investigation, Indian Evidence Act, Bharatiya Sakshya Adhiniyam, Electronic Records, Hash Value, Cloud Forensics.*

ISSN: 2582-6433

2. INTRODUCTION

The digital revolution has fundamentally transformed the landscape of criminal activity and law enforcement alike. Crimes that were once confined to physical spaces now occur across invisible electronic networks spanning continents and jurisdictions. The proliferation of smartphones, personal computers, cloud computing infrastructure, social media platforms, and the Internet of Things (IoT) has created an almost inexhaustible reservoir of digital traces traces that, when properly identified and preserved, constitute evidence of the highest probative value.[1]

Cyber forensics, as a discipline, emerged from the urgent practical necessity of investigating computer-related crimes. Its origins may be traced to the late 1970s and early 1980s, when law enforcement agencies in the United States first encountered criminal misuse of personal computers.[2] The field has since evolved into a highly specialised and technically sophisticated discipline, governed by internationally recognised standards and increasingly codified in national legislation.

In India, the legal framework governing cyber forensics is still in a relatively nascent stage of development, though significant strides have been made in the past two decades. The Information Technology Act, 2000 (hereinafter "IT Act") constituted a watershed moment in the recognition of electronic records and digital evidence under Indian law.[3] The amendment of 2008 further broadened the scope of the statute to address emerging categories of cybercrime and refined the evidentiary provisions relating to digital records. The recent enactment of the Bharatiya Sakshya Adhiniyam, 2023 (hereinafter "BSA") and the Bharatiya Nagarik Suraksha Sanhita, 2023 (hereinafter "BNSS") represents the most comprehensive overhaul of the evidentiary and procedural law in post-independence India, with significant implications for cyber forensic practice.[4]

This article proceeds in fourteen parts. Following this introduction, the article delineates the

[1] Nir Kshetri, The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives 3 (Springer 2010); see also Casey Eoghan, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet 1 (3rd ed., Academic Press 2011).
[2] Eoghan Casey, Handbook of Digital Forensics and Investigation 1–5 (Academic Press 2010); Mark M. Pollitt, A History of Digital Forensics, in Advances in Digital Forensics VI 3 (Kam-Pui Chow & Sujeet Shenoi eds., Springer 2010).
[3] Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India) [hereinafter IT Act].
[4] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023 [hereinafter BSA]; Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023 [hereinafter BNSS]; Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 [hereinafter BNS].

ISSN: 2582-6433

conceptual framework of cyber forensics (Part II), traces its historical evolution in India (Part III), and provides a detailed analysis of the Indian statutory framework (Part IV). Parts V through VII examine the legal dimensions of digital evidence, chain of custody, and forensic methodology. Part VIII addresses specific categories of cybercrime, while Part IX analyses landmark judicial precedents. Parts X and XI situate Indian cyber forensic law within the comparative international context and examine the institutional framework. Part XII addresses emerging technological challenges, and Parts XIII and XIV offer critical analysis, legislative recommendations, and conclusions.[5]

3. CONCEPTUAL FRAMEWORK OF CYBER FORENSICS

Cyber forensics, as defined by the Scientific Working Group on Digital Evidence (SWGDE), is "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of information and maintaining a strict chain of custody for the data."[6] The definition adopted by the Association of Chief Police Officers (ACPO) of the United Kingdom identifies digital forensics as the recovery and investigation of material found in digital devices, often in relation to computer crime.[7]

The scope of cyber forensics is broader than mere computer forensics and encompasses the investigation of all digital devices, platforms, and media, including: (a) computer systems and hard disks; (b) mobile and handheld devices; (c) network infrastructure; (d) cloud storage environments; (e) social media platforms and online services; (f) IoT devices; and (g) embedded systems. Each of these categories presents distinct technical and legal challenges in the forensic investigation process.[8]

The discipline of cyber forensics comprises several specialised branches. **Computer Forensics** concerns the recovery and analysis of data from computer systems, hard drives, and removable storage media. **Network Forensics** involves the monitoring and analysis of computer network

[5] The methodology adopted in this article is primarily doctrinal, employing textual analysis of primary legal sources supplemented by analytical and comparative approaches. See generally Terry Hutchinson & Nigel Duncan, Defining and Describing What We Do: Doctrinal Legal Research, 17 Deakin L. Rev. 83 (2012).

[6] Scientific Working Group on Digital Evidence (SWGDE), Recommendations for Digital, Multimedia, and Computer Forensics (SWGDE Working Group 2012), available at https://www.swgde.org.

[7] Association of Chief Police Officers (ACPO), Good Practice Guide for Digital Evidence (4th ed. 2008), at para. 1.3.

[8] National Institute of Justice, U.S. Dep't of Justice, Electronic Crime Scene Investigation: A Guide for First Responders (2d ed. 2008); see also Andrew Jones & Craig Valli, building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility 15 (Butterworth-Heinemann 2009).

ISSN: 2582-6433

traffic for the purposes of information gathering, legal evidence collection, or intrusion detection.[9]

Mobile Device Forensics is concerned with the extraction and analysis of data from mobile phones, tablets, and GPS devices. **Database Forensics** focuses on the forensic study of databases and their metadata. **Cloud Forensics**, an emerging branch, addresses the unique challenges of investigating crimes involving cloud computing environments, including issues of multi-tenancy, jurisdiction, and volatility of evidence.[10]

Malware Forensics involves the identification, analysis, and documentation of malicious software. **Email Forensics** concerns the recovery and analysis of electronic mail as evidence. **Memory Forensics** addresses the acquisition and analysis of data from volatile memory (RAM), which may contain evidence of running processes, encryption keys, and network connections that would otherwise be lost upon system shutdown.[11]

The conduct of cyber forensic investigations is governed by several fundamental principles that are both scientifically necessary and legally mandated. The **Principle of Integrity** requires that the original digital evidence must not be altered during the investigation process. Forensic investigators employ write-blockers and create bit-by-bit copies (forensic images) to ensure that original media remains unmodified.[12]

The **Principle of Reproducibility** mandates that forensic processes must be reproducible; a different forensic examiner, applying the same methodology to the same evidence, must arrive at the same result. The **Principle of Documentation** requires that every step of the forensic investigation be meticulously documented, creating a comprehensive audit trail that can withstand scrutiny in adversarial legal proceedings.[13]

The **Locard Exchange Principle**, originally formulated in the context of physical forensic science by Dr. Edmond Locard, holds that "every contact leaves a trace." In the digital context,

[9] Albert Marcella, Jr. & Doug Menendez, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes 45 (2d ed., Auerbach Publications 2008).
[10] Josiah Dykstra & Alan T. Sherman, Design and Implementation of FROST: Digital Forensic Tools for the OpenStack Cloud Computing Platform, 68 Digital Investigation S87 (2013).
[11] Lenny Zeltser, Network Forensic Analysis, in Incident Response: Investigating Computer Crime 191 (Kevin Mandia, Chris Prosise & Matt Pepe eds., McGraw-Hill Osborne Media 2003).
[12]Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet 177 (3rd ed., Academic Press 2011).

ISSN: 2582-6433

this principal manifests in the observation that virtually every interaction with a digital system leaves behind traces log files, metadata, registry entries, cache data that can be recovered and analysed by competent forensic investigators.[13]

4. DIGITAL EVIDENCE: ADMISSIBILITY AND EVIDENTIARY STANDARDS

Digital evidence is inherently distinct from traditional documentary or physical evidence in several material respects. It is intangible, existing as patterns of electrical charges or magnetic states. It is fragile; it can be easily altered, deleted, or corrupted, often without any visible sign of tampering. It is volatile; certain forms of digital evidence, particularly data held in RAM, exist only as long as the system remains powered. It is voluminous, often requiring the analysis of gigabytes or terabytes of data. It may be encrypted, requiring specialised tools or knowledge to access. And it may be located across multiple jurisdictions simultaneously, creating complex issues of sovereignty and mutual legal assistance.[14]

Digital evidence may be categorised in several ways. From a forensic perspective, the most useful categorisation distinguishes between: (1) **Active data** files and data that are currently in use and immediately accessible; (2) **Archival data** data that has been archived for long-term storage; (3) **Residual data (latent data)** data that has been deleted from active storage but remains recoverable through forensic techniques; and (4) **Metadata** data about data, including information about when a file was created, modified, accessed, and by whom.[15]

A. Admissibility under Indian Law: The Section 63 BSA Framework

As noted above, the admissibility of electronic records under Indian law is governed primarily by Section 63 of the BSA (formerly Section 65B of the Indian Evidence Act). The conditions specified in Section 63 are both substantive and procedural. Non-compliance with these conditions renders the electronic evidence inadmissible, regardless of its intrinsic probative value or authenticity.[16]

The Supreme Court in Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 authoritatively held that

[13]Brian Carrier, File System Forensic Analysis 5–10 (Addison-Wesley Professional 2005); see also Garfinkel Simson, Digital Forensics Research: The Next 10 Years, 7 Digital Investigation S64 (2010).
[14] Edmond Locard, L'enquête criminelle et les méthodes scientifiques (Flammarion 1920); see adaptation for digital forensics in Casey, supra note 12, at 15.
[15] Pawan Duggal, Cyberlaws: The Indian Perspective 1–20 (Saakshar Law Publications 2002); Talat Fatima, Cybercrimes 35 (Eastern Book Company 2011).
[16] BSA, supra note 4, § 63.

ISSN: 2582-6433

electronic evidence is admissible only if accompanied by a certificate satisfying the requirements of Section 65B. The court specifically rejected the argument that such records could be admitted under the general provisions relating to secondary evidence (Sections 63–65 of the IEA). This position was reaffirmed and elaborated in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1, where the court provided further clarity on who is competent to issue the certificate and the circumstances in which it must be produced.[17]

B. Authentication and Verification of Digital Evidence

The authentication of digital evidence is a central concern of cyber forensic practice. Authentication refers to the process of establishing that the evidence is what it purports to be that a purported email was in fact sent from a particular account, that a document was created at a particular time, or that a particular piece of code constitutes the malware alleged to have been used in an attack. Hash value verification is the primary technical mechanism employed for this purpose.[18]

A cryptographic hash function generates a unique fixed-length digital "fingerprint" of a file or dataset. The most commonly used hash functions in forensic practice are MD5 (Message Digest 5) and SHA-256 (Secure Hash Algorithm 256-bit). If even a single bit of data is altered in the original file, the hash value will change completely. By computing the hash value of the original evidence at the time of seizure and comparing it with the hash value of the forensic copy at the time of analysis and production before the court, investigators can demonstrate that the evidence has not been altered.[19]

C. Hearsay Rule and Electronic Evidence

The application of the hearsay rule to electronic evidence is a nuanced issue. Under English common law (and to a large extent under Indian evidence law), out-of-court statements tendered for the truth of their contents are generally inadmissible as hearsay. The question arises whether computer-generated records constitute hearsay evidence. Indian courts have generally taken the position, consistent with the approach adopted in England, that automatically generated computer records (such as system logs and traffic data) are not hearsay because they do not involve any human declarant; they are generated by a machine following its programmed instructions. Human-input records (such as word-processed documents or

[17] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India); Arjun Panditrao Khotkar, (2020) 7 SCC 1 (India).
[18] Casey, supra note 12, at 177–180.
[19] National Institute of Standards & Technology, Digital Signatures: MD5 and SHA-256 (NIST FIPS PUB 180-4, 2015).

ISSN: 2582-6433

emails) may, however, raise hearsay issues that must be addressed through appropriate exceptions.[20]

5. THE CHAIN OF CUSTODY IN CYBER FORENSIC INVESTIGATIONS

A. Legal Significance of Chain of Custody

The chain of custody is a legal concept that refers to the chronological documentation or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. A properly maintained chain of custody is essential for ensuring the admissibility of evidence in legal proceedings and for establishing the integrity and authenticity of the evidence. Any gap or irregularity in the chain of custody can provide a basis for the opposing party to challenge the admissibility or reliability of the evidence.[21]

In the context of digital evidence, maintaining an unbroken chain of custody is particularly challenging due to the intangible nature of the evidence and the technical complexity of the processes involved. Indian courts have consistently emphasised the importance of a proper chain of custody for digital evidence. In State (NCT of Delhi) v. Navjot Sandhu (the Parliament Attack Case), the Supreme Court, while admitting certain electronic evidence despite procedural irregularities, noted the importance of establishing the authenticity and integrity of digital records.[22]

B. Procedural Requirements for Chain of Custody

A proper chain of custody for digital evidence requires: (1) the contemporaneous documentation of the seizure of the device, including the date, time, location, and the identity of the seizing officer; (2) the creation of a forensic image of the device, with hash value verification, before any analysis is conducted; (3) the secure storage of the original device in a manner that prevents contamination or alteration; (4) the documentation of every access to the evidence, including the purpose, the identity of the person accessing, and the duration of access; (5) the maintenance of a forensic examination log documenting every tool and technique applied; and (6) the secure transfer of evidence between custodians with documentary acknowledgement at each stage.[23]

Section 176(3) of the BNSS, which mandates the videography of searches, provides a

[20] Mason & Seng, supra note 39, at 71–95; see also R v. Shepherd [1993] AC 380 (HL) (England) (on computerised records and the hearsay rule).
[21] Casey, supra note 12, at 200
[22] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600, ¶ 150 (India).
[23] NIST SP 800-86, supra note 40, at 3-1 to 3-5.

ISSN: 2582-6433

significant statutory reinforcement of the chain of custody requirements for digital evidence in India. The mandated video record creates a contemporaneous visual corroboration of the circumstances of seizure that is difficult to challenge and provides courts with direct evidence of the manner in which the digital evidence was obtained.[24]

C. Consequences of a Broken Chain of Custody

A broken or inadequately documented chain of custody may result in the exclusion of digital evidence from trial, significantly weakening or even fatally undermining the prosecution's case. Even where the court does not exclude the evidence, a demonstrably weak chain of custody will diminish the evidentiary weight that the court accords to the evidence and provide the defence with powerful ammunition for cross-examination. Indian courts have held that while a minor irregularity in the chain of custody does not necessarily render evidence inadmissible, a material breach that raises a reasonable doubt about the integrity of the evidence may justify exclusion.[25]

6. CYBER FORENSIC METHODOLOGY: LEGAL IMPLICATIONS

A. The Forensic Investigation Process

The cyber forensic investigation process comprises several distinct phases, each with its own legal implications. The first phase, **Identification**, involves recognising potential evidence sources and determining the scope of the investigation. This phase is governed by the legal basis for the investigation whether it is a court-ordered search, a consensual examination, or an administrative enquiry.[26]

The second phase, **Collection**, involves the physical or logical acquisition of electronic evidence. This phase is the most critical from a legal standpoint, as it is here that the foundational requirements of admissibility including chain of custody and integrity preservation must be established. Indian law, through Sections 94 and 105 of the BNSS, provides the legal authority for the seizure of electronic devices and records.[27]

The third phase, **Preservation**, requires that the integrity of the collected evidence be maintained through appropriate technical measures. The fourth phase, **Examination and**

[24] BNSS, supra note 4, § 176(3).
[25] Trimukh Maroti Kirkan v. State of Maharashtra, (2006) 10 SCC 681 (India) (on the consequences of a defective chain of custody).
[26] Ryan Ko et al., Cloud Computing and Digital Forensics, in Digital Forensics and Cyber Crime 201 (Sanjay Goel ed., Springer 2013).
[27] [87] DPDPA, supra note 38; BNSS, supra note 4, § 94.

ISSN: 2582-6433

Analysis, involves the application of forensic tools and techniques to extract and interpret evidentiary data from the preserved evidence. The fifth phase, **Documentation and Reporting**, culminates in the production of a forensic examination report that can be presented to courts and withstand adversarial scrutiny.[28]

B. Forensic Tools and Legal Validity

The legal validity of the results produced by cyber forensic tools has been a recurring issue in Indian courts. Commonly used forensic tools include EnCase (by OpenText), FTK (Forensic Tool Kit by Access Data/Exterro), Autopsy, Cellebrite UFED (for mobile devices), and AXIOM. For these tools to produce legally admissible results, they must be shown to be reliable, validated, and applied correctly by competent forensic examiners.[29]

Indian courts have, in several cases, admitted expert testimony from forensic examiners regarding the tools used and the results obtained. However, the absence of a mandatory accreditation or certification framework for cyber forensic tools in India is a significant lacuna. In contrast, the United States employs the Daubert standard and its Indian equivalent the common law test of reliability, relevance, and helpfulness to evaluate the admissibility of scientific evidence, including cyber forensic evidence.[30]

C. First Responder Protocols

The conduct of first responders typically police officers who are the first to arrive at a crime scene involving electronic evidence is critically important. Improper handling by first responders can irreparably compromise digital evidence. The most common errors committed by inadequately trained first responders include: switching on powered-off devices (which can alter the file system and metadata); switching off running devices (which can destroy volatile evidence in RAM); browsing the file system of a seized computer without creating a forensic image; and failure to photograph and document the state of the scene before any interaction.[31]

The Ministry of Home Affairs, Government of India, has issued guidelines for first responder protocols in cybercrime investigations. However, these guidelines do not have statutory force and their implementation across different state police forces is uneven. The absence of

[28] Ralph Brewer & Monica Swiatek, Forensics in the Internet of Things, in Handbook of Digital Forensics 350 (Vassil Roussev ed., Springer 2016).
[29] Ralph Brewer & Monica Swiatek, Forensics in the Internet of Things, in Handbook of Digital Forensics 350 (Vassil Roussev ed., Springer 2016).
[30] Steve Larson et al., Artificial Intelligence in Digital Forensics: A Review, 27 J. Forensic Sci. 1122 (2022).
[31] Victor Kebande & Indrakshi Ray, A Generic Digital Forensic Investigation Framework for Internet of Things (IoT), in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud 561 (2016).

ISSN: 2582-6433

mandatory statutory training and certification requirements for cyber-crime first responders is a significant deficiency in the Indian cyber forensic framework.

7. SPECIFIC CATEGORIES OF CYBERCRIME AND FORENSIC CHALLENGES

A. Financial Cybercrime and Cryptocurrency Fraud

Financial cybercrime, encompassing bank fraud, online payment fraud, phishing, business email compromise, and investment scams, represents the most prevalent category of cybercrime in India and globally. The investigation of financial cybercrime presents specific forensic challenges, including the tracing of funds through multiple accounts and financial intermediaries, the analysis of communication records, and the recovery of deleted transaction data.[32]

Cryptocurrency fraud poses particularly acute forensic challenges. Unlike traditional financial transactions, cryptocurrency transactions are pseudonymous and occur on a decentralised blockchain without the involvement of a traditional financial intermediary. The investigation of cryptocurrency fraud requires specialised blockchain analytics tools (such as Chain analysis, Elliptic, and Cipher Trace) and expertise in tracing transactions through mixing services and chain-hopping techniques. Indian law currently lacks a specific regulatory framework for cryptocurrency forensics, though the Prevention of Money Laundering Act, 2002 has been extended to cover virtual digital assets.[33]

B. Cyberterrorism and National Security

Section 66F of the IT Act defines and penalises the offence of cyber terrorism as the commission of any act with intent to threaten the unity, integrity, security, or sovereignty of India or to strike terror in the people or any section of the people by: (a) denying or causing the denial of access to any person authorised to access any computer resource; (b) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or (c) introducing or causing the introduction of any computer contaminant.[34]

The investigation of cyber terrorism offences necessarily involves the collection of evidence from multiple jurisdictions and platforms, often requiring formal mutual legal assistance. The

[32] Norton by Symantec, Norton Cyber Security Insights Report (2017); Reserve Bank of India, Annual Report on Banking and Financial Frauds (2023).
[33] PMLA, supra note 37; Ministry of Finance, Govt. of India, Prevention of Money Laundering (Maintenance of Records) Amendment Rules, 2023 (extending PMLA to virtual digital assets).
[34] IT Act, supra note 3, § 66F.

ISSN: 2582-6433

National Security Council Secretariat and the National Technical Research Organisation (NTRO) are among the agencies involved in cyber intelligence and the forensic investigation of national security-related cyber incidents. The evidentiary challenges in cyber terrorism cases are compounded by the use of encryption, anonymisation tools, and the Tor network by sophisticated threat actors.[35]

C. Cyberstalking, Online Harassment, and CSAM

Cyberstalking and online harassment are addressed in India primarily under Section 354D of the IPC (now the BNS) and Section 66E and Section 67 of the IT Act. The forensic investigation of these offences requires the collection and analysis of communication records (messages, emails, social media interactions), IP address logs, device location data, and metadata from images and videos. The challenges include: obtaining legal process from foreign platforms; preserving ephemeral messaging data; and handling encrypted end-to-end communications.[36]

The investigation of child sexual abuse material (CSAM) under Section 67B of the IT Act is a matter of the gravest legal and ethical sensitivity. Forensic examiners dealing with CSAM must comply with strict protocols to minimise exposure to the material and must ensure that recovered material is handled in a manner consistent with victim dignity. The National Centre for Missing and Exploited Children (NCMEC) in the United States operates the CyberTipline, which receives reports from electronic service providers and shares information with law enforcement globally, including in India.[37]

D. Data Breaches and Corporate Espionage

Data breaches and corporate espionage cases present complex forensic challenges, including the identification of intrusion vectors, the attribution of attacks to specific threat actors, the quantification of data exfiltration, and the recovery of logs and artifacts that can establish the timeline of the attack. The investigation of these offences involves the analysis of network logs, intrusion detection system (IDS) data, endpoint detection and response (EDR) telemetry, and system event logs.[38]

Indian law, under Sections 43, 66, and 72 of the IT Act, provides civil and criminal remedies

[35] Saikat Datta, The Spy Chronicles: RAW, ISI and the Illusion of Peace 210 (HarperCollins India 2018).
[36] IPC, supra note 35, § 354D; IT Act, supra note 3, §§ 66E, 67.
[37] IT Act, supra note 3, § 67B; POCSO, supra note 37; National Centre for Missing & Exploited Children, CyberTipline 2022 Report (2023
[38] Mandiant, M-Trends 2023: Special Report 5 (2023).

ISSN: 2582-6433

for unauthorised access and data theft. However, the absence of a comprehensive data protection law with specific provisions for forensic investigation of data breaches has been a significant lacuna, which the Digital Personal Data Protection Act, 2023, seeks to partially address. The DPDPA imposes mandatory breach notification obligations on data fiduciaries, which will generate additional digital evidence in the form of breach reports and compliance records.[39]

8. JUDICIAL PRECEDENTS AND CASE LAW

A. Landmark Supreme Court Decisions

1. State (NCT of Delhi) v. Navjot Sandhu (2005)

In the landmark Parliament Attack Case, the Supreme Court of India, while convicting the accused for criminal conspiracy and waging war against the Government of India in connection with the attack on the Indian Parliament on 13 December 2001, admitted electronic evidence in the form of call detail records (CDRs) without strict compliance with the Section 65B certification requirement. The court held that secondary evidence of electronic records could be admitted under Sections 63 and 65 of the Indian Evidence Act.[40]

This decision, while subsequently overruled on the question of the admissibility of electronic evidence in Anvar P.V. v. P.K. Basheer, remains significant as a demonstration of the courts' willingness to adapt traditional evidentiary rules to the requirements of digital evidence in high-stakes cases. The decision also touched on important questions regarding the evidentiary value of voice recordings and the identification of voices.[41]

2. Anvar P.V. v. P.K. Basheer (2014)

This decision of a three-judge bench of the Supreme Court of India constitutes the most important judicial pronouncement on the admissibility of electronic evidence under Indian law. The case arose from an election petition in Kerala, where the petitioner sought to adduce electronic evidence in the form of a CD recording and printouts from a website. The court held, overruling the Navjot Sandhu decision on this point, that electronic evidence is admissible only if accompanied by a certificate meeting the requirements of Section 65B of the Indian Evidence Act, 1872.[42]

The decision in Anvar P.V. established several critical principles: (a) that electronic records

[39] IT Act, supra note 3, §§ 43, 66, 72; DPDPA, supra note 38, § 8(6) (breach notification obligation).
[40] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
[41] Id. at ¶¶ 148–157.
[42] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶ 24 (India).

ISSN: 2582-6433

can only be proved in accordance with Section 65B and not under any other provision of the Evidence Act; (b) that the certificate under Section 65B is a condition precedent for admissibility; (c) that the certificate must be given by a person who is in a "responsible official position" in relation to the operation of the device; and (d) that original evidence does not require a certificate but secondary evidence (i.e., a copy) invariably does.[43]

3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

This decision of a three-judge bench of the Supreme Court clarified several ambiguities arising from the Anvar P.V. decision. The court held that: (a) the certificate under Section 65B is mandatory for secondary electronic evidence; (b) where the certificate has not been produced by the party relying on the electronic evidence, the court may give such party an opportunity to produce the certificate; (c) the certificate need not be produced at the time of filing the electronic evidence but must be produced before the court relies on it; and (d) if the certificate cannot be obtained from the relevant person, the court may issue a direction requiring the relevant person to produce it.[44]

4. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

In this landmark nine-judge bench decision, the Supreme Court unanimously recognised the right to privacy as a fundamental right protected under Article 21 of the Constitution of India. While not directly a cyber forensics case, the Puttaswamy decision has profound implications for cyber forensic practice, establishing constitutional limits on the State's power to intercept, monitor, and access the digital communications and data of citizens. The judgment requires that any exercise of the powers conferred by Sections 69–69B of the IT Act must satisfy the tests of legality, necessity, and proportionality.[45]

5. Shreya Singhal v. Union of India (2015)

In Shreya Singhal, the Supreme Court struck down Section 66A of the IT Act as unconstitutional on the ground that the provision violated the right to freedom of speech and expression guaranteed by Article 19(1)(a) of the Constitution. The court held that the terms used in Section 66A "grossly offensive," "menacing," "causing annoyance," and the like were vague, overbroad, and capable of chilling legitimate speech. The decision also addressed Section 79 of the IT Act, holding that the safe harbour provision for intermediaries is constitutionally valid.[46]

[43] Id. at ¶¶ 14–24.
[44] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, ¶¶ 49–55 (India).
[45] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[46] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

ISSN: 2582-6433

B. Significant High Court Decisions

Several High Courts have contributed importantly to the development of Indian cyber forensic law. The Kerala High Court, in Shafhi Mohammad v. State of Kerala, considered whether the requirement of a Section 65B certificate applied to forensic examination reports produced by government forensic scientists. The court held that government forensic scientists are in a "responsible official position" for the purposes of Section 65B and can therefore issue the requisite certificate.[47]

The Delhi High Court, in Dharambir v. Central Bureau of Investigation, addressed questions regarding the admissibility of CDR data, holding that CDRs are electronic records under Section 2(1)(t) of the IT Act and must be accompanied by a Section 65B certificate to be admissible as secondary evidence. The Bombay High Court, in several cases concerning financial cybercrime, has addressed questions of jurisdiction in cases where the offence was committed using servers located in foreign jurisdictions.[48]

9. COMPARATIVE INTERNATIONAL PERSPECTIVES

A. The United States

The United States provides one of the most developed legal frameworks for cyber forensic investigations. The primary federal statutes governing cyber forensics are the Computer Fraud and Abuse Act, 1986 (CFAA), the Electronic Communications Privacy Act, 1986 (ECPA), the Stored Communications Act (SCA), and the USA PATRIOT Act, 2001. The Federal Rules of Evidence (FRE) govern the admissibility of digital evidence, with Rule 901 addressing authentication requirements and Rule 702 governing the admissibility of expert testimony applying the Daubert standard.[49]

The National Institute of Standards and Technology (NIST) has published comprehensive guidelines for cyber forensic investigations, including the NIST Special Publication 800-86 (Guide to Integrating Forensic Techniques into Incident Response) and SP 800-101 (Guidelines on Mobile Device Forensics). These guidelines, while not legally binding, are widely adopted by law enforcement and private sector forensic practitioners as best practice standards.[50]

[47] Shafhi Mohammad v. State of Kerala, (2018) 2 SCC 801 (India).
[48] Dharambir v. Central Bureau of Investigation, (2008) 82 DRJ 655 (Del. HC) (India).
[49] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2523 (1986); Stored Communications Act, 18 U.S.C. §§ 2701–2713 (1986); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[50] NIST SP 800-86, supra note 40; NIST Special Publication 800-101, Revision 1: Guidelines on Mobile Device Forensics (Wayne Jansen & Rick Ayers eds., 2014).

ISSN: 2582-6433

B. The European Union

The European Union's approach to cyber forensics is shaped by the General Data Protection Regulation (GDPR), 2016, the Directive on Attacks Against Information Systems (2013/40/EU), and the proposed Regulation on Electronic Evidence (e-Evidence Regulation), which, when adopted, will create a cross-border framework for law enforcement authorities to directly request electronic evidence from service providers in other EU Member States.[51]

The GDPR's provisions relating to the processing of personal data have direct implications for cyber forensic investigations, as the collection and analysis of digital evidence often necessarily involves the processing of personal data. Law enforcement in EU Member States must navigate the tension between the requirements of the GDPR and the needs of criminal investigations, a challenge that India will increasingly face as its own data protection regime matures.[52]

C. The Budapest Convention on Cybercrime

The Convention on Cybercrime (the Budapest Convention), adopted by the Council of Europe in 2001, is the first international treaty on crimes committed via the Internet and other computer networks. It addresses cybercrime substantive law, procedural provisions (including expedited preservation of data, production orders, search and seizure of computer data, real-time collection of traffic data, and interception of content data), and international cooperation mechanisms. As of April 2026, 68 states have ratified the Convention.[53]

India is not a signatory to the Budapest Convention, a position that has attracted considerable criticism from cybersecurity scholars and law enforcement practitioners. India's non-participation in the Budapest Convention significantly impedes its ability to leverage the Convention's international cooperation mechanisms, particularly the 24/7 network of contact points for expedited assistance in cybercrime investigations. While India relies upon bilateral Mutual Legal Assistance Treaties (MLATs) for international cyber-crime cooperation, these mechanisms are considerably slower and less efficient than the Convention's frameworks.[54]

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L 119/1; Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems [2013] OJ L 218/8.

[52] Article 29 Working Party, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (EU 2018); see also GDPR arts. 4(2), 6.

[53] Council of Europe, Convention on Cybercrime, CETS No. 185 (Budapest, 23 Nov. 2001) [hereinafter Budapest Convention], available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[54] Praveen Dalal, Cyber Law in India 415 (1st ed., Saakshar Law Publications 2011); cf. Budapest Convention, supra note 79, art. 35 (24/7 network).

ISSN: 2582-6433

10. INSTITUTIONAL FRAMEWORK: AGENCIES AND AUTHORITIES

A. Indian Computer Emergency Response Team (CERT-In)

CERT-In, established under Section 70B of the IT Act, functions as the national nodal agency for computer security incident response. CERT-In is responsible for collecting, analysing, and disseminating information on cyber incidents; issuing forecasts and alerts; coordinating emergency measures in the event of cyber security incidents; coordinating activities relating to cyber security emergency measures and crisis management; providing technical assistance and advice to entities; and creating a national repository of information on cyber-crime. CERT-In also plays a role in the forensic analysis of certain categories of cyber incidents, particularly those affecting critical information infrastructure.

B. National Cyber Crime Reporting Portal

The National Cyber Crime Reporting Portal (cybercrime.gov.in) was established by the Ministry of Home Affairs to enable citizens to report cyber-crimes online. The portal is specifically designed for reporting cyber crimes against women and children, and financial crimes. The Indian Cyber Crime Coordination Centre (I4C), which administers the portal, coordinates the investigation of cybercrime across state police forces and provides technical support for cyber forensic investigations.

C. Central Forensic Science Laboratories

The Central Forensic Science Laboratory (CFSL), functioning under the Directorate of Forensic Science Services (DFSS) of the Ministry of Home Affairs, operates laboratories in Hyderabad, Kolkata, Chandigarh, Pune, and Bhopal. Each CFSL has a specialised Cyber Forensic Division (CFD) equipped to conduct forensic examination of digital devices, recover deleted data, analyse malware, and produce expert forensic reports for submission to courts. The examination reports produced by CFSL scientists are treated by Indian courts as expert opinions and are entitled to significant evidentiary weight.

D. CBI Cyber Crime Investigation Cell

The Central Bureau of Investigation (CBI) operates a specialised Cyber Crime Investigation Cell (CCIC) for the investigation of complex and high-profile cybercrime cases. The CCIC is equipped with advanced digital forensic capabilities and maintains liaison with international law enforcement agencies, including Interpol and the US Federal Bureau of Investigation (FBI), for cross-border cybercrime investigations. The CBI also operates a Cyber Crime Unit

ISSN: 2582-6433

in its Special Crimes Division for the investigation of cyberterrorism and national security-related cyber offences.

11. CRITICAL ANALYSIS AND LEGISLATIVE GAPS

India currently lacks a comprehensive statute specifically dedicated to the regulation of cyber forensic investigations. The relevant provisions are scattered across the IT Act, the BSA, the BNSS, the BNS, and a range of subsidiary legislation and administrative guidelines. This fragmentation creates inconsistencies, ambiguities, and gaps that impede the effective investigation and prosecution of cybercrime. A dedicated Cyber Forensics and Digital Evidence Act, modelled on the approach taken in countries such as the United Kingdom (Police and Criminal Evidence Act, 1984, as supplemented by the ACPO Guidelines and the Forensic Science Regulator's Codes of Practice) would significantly enhance legal clarity and procedural certainty.

Indian law does not currently mandate the validation or certification of cyber forensic tools used in criminal investigations. This stands in contrast to the approach adopted in many jurisdictions, where forensic tools must meet specific technical standards before their results can be admitted in criminal proceedings. The absence of such requirements creates a risk that inaccurate or unreliable forensic results may be produced and admitted without adequate scrutiny, potentially resulting in miscarriages of justice.[95]

A significant challenge in the Indian cyber forensic ecosystem is the inadequacy of training and capacity at the operational level. While elite forensic laboratories such as CFSL and specialised units such as the CBI CCIC possess advanced capabilities, the majority of state police forces lack the technical expertise, equipment, and resources required for competent cyber forensic investigation. The result is that many cyber-crime cases are inadequately investigated, and digital evidence that could be critical to prosecution is lost through improper handling.

The training of judicial officers is equally important. Judges adjudicating cyber crime cases must possess sufficient technical literacy to evaluate competing expert testimony regarding digital evidence, assess the validity of forensic methodologies, and make informed decisions on the admissibility and weight of electronic records. The National Judicial Academy and State Judicial Academies have begun to address this need through specialised training programmes,

ISSN: 2582-6433

but much more remains to be done.

Cybercrime is inherently transnational in character, and the effective investigation of many categories of cybercrime requires cooperation between law enforcement agencies of multiple countries. India's existing mechanisms for international cooperation in cybercrime investigations primarily bilateral MLATs and the Interpol system are slow and cumbersome. India's non-membership of the Budapest Convention and the absence of a domestic framework for expedited preservation and production of foreign digital evidence significantly hampers the effective investigation of transnational cybercrime.

The powers conferred by Sections 69–69B of the IT Act for interception, monitoring, and decryption of digital communications and data are extremely broad and are not subject to independent judicial oversight of the kind that exists in many other jurisdictions. The Supreme Court's recognition of the right to privacy as a fundamental right in the Puttaswamy case provides a constitutional basis for challenging disproportionate exercises of these powers. However, the absence of a comprehensive surveillance reform legislation in India, despite the Puttaswamy judgment, remains a matter of serious concern for civil liberties advocates and legal scholars.

12. CONCLUSION AND RECOMMENDATIONS

This research article has examined the conceptual, technical, and legal dimensions of cyber forensics in the Indian context. It has demonstrated that while India has made significant strides in the development of a legal framework for cyber forensics particularly through the IT Act, the new criminal laws of 2023, and a growing body of judicial precedent substantial gaps and challenges remain. The fragmentation of the legal framework, the inadequacy of forensic tool validation standards, the lack of comprehensive first responder protocols with statutory force, the challenges of cloud and IoT forensics, and the absence of effective international cooperation mechanisms are among the most pressing concerns.

India should enact a dedicated statute governing cyber forensic investigations, consolidating the currently fragmented provisions and providing clear guidance on collection, preservation, analysis, and presentation of digital evidence. Such a statute should include provisions on forensic tool certification, first responder training, chain of custody documentation, and expert witness qualification.

ISSN: 2582-6433

India should seriously consider acceding to the Budapest Convention on Cybercrime, which would significantly enhance India's capacity for international cooperation in cybercrime investigations and provide access to the Convention's expedited evidence-preservation and production mechanisms.

The National Judicial Academy and State Judicial Academies should develop mandatory specialised training programmes for judges on the technical aspects of digital evidence and cyber forensics, ensuring that the judiciary can effectively evaluate expert testimony and make informed evidentiary rulings in cybercrime cases.

A comprehensive surveillance reform legislation should be enacted to provide for independent judicial oversight of the exercise of powers of interception, monitoring, and decryption under the IT Act, ensuring compliance with the proportionality requirements established in the Puttaswamy decision.

CERT-In and the Bureau of Indian Standards (BIS) should collaborate with industry and academic experts to develop national standards for cloud forensics and IoT forensics, providing forensic investigators with a reliable methodological framework for the investigation of crimes involving these technologies.

The rapid evolution of digital technology continuously reshapes the terrain of criminal activity and forensic investigation. The legal framework governing cyber forensics must evolve in tandem with this technological change, providing investigators with adequate legal authority while safeguarding the rights of citizens and maintaining the integrity of the justice system. India's legal framework for cyber forensics, though significantly advanced in recent years, must continue to develop through thoughtful legislation, judicial elaboration, and institutional capacity building if it is to meet the challenges of the digital age.

The intersection of law and technology in the field of cyber forensics is one of the most dynamic and consequential areas of contemporary legal scholarship. It demands the sustained attention of legislators, jurists, legal scholars, and forensic practitioners. The recommendations proposed in this article, if implemented, would significantly strengthen India's capacity to investigate and prosecute cybercrime effectively and equitably, contributing to a safer and more secure digital environment for all citizens.