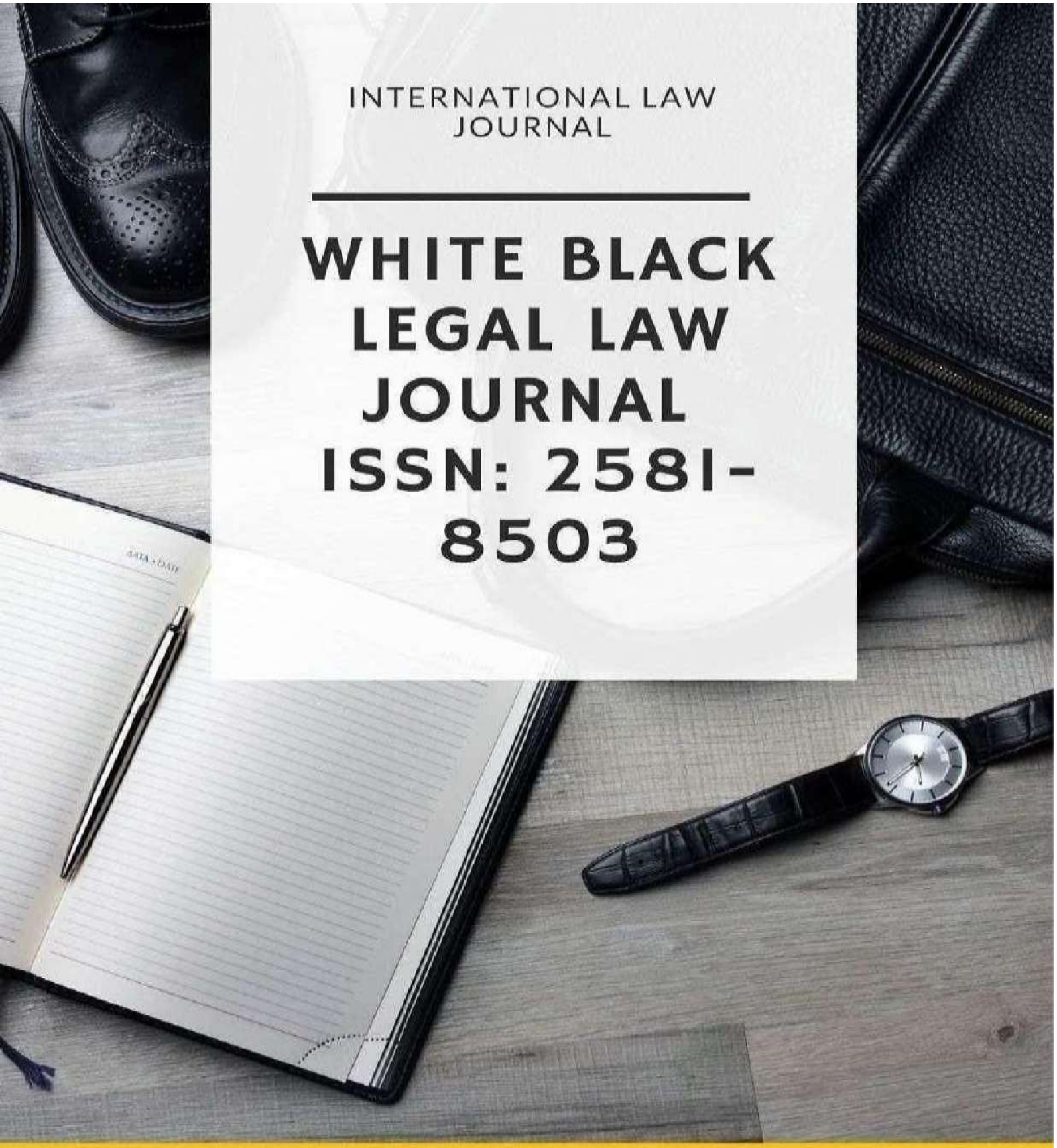

INTERNATIONAL LAW JOURNAL

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.

ELECTRONIC EVIDENCE IN INDIAN JURISPRUDENCE: EVOLUTION, CONCEPTUAL FRAMEWORK, AND CONTEMPORARY CHALLENGES

AUTHORED BY - SAMARTH SAXENA

Abstract

The digital transformation of contemporary society has fundamentally altered the nature of evidence presented in legal proceedings. As electronic records increasingly replace traditional paper-based documents in both civil and criminal trials, the Indian legal system has been compelled to adapt its evidentiary framework to accommodate the unique characteristics and challenges of digital proof. This paper traces the evolution of the law of electronic evidence in India, beginning with the paper-based documentary evidence framework under the Indian Evidence Act, 1872, through the early judicial encounters with tape-recorded evidence, to the watershed amendments introduced by the Information Technology Act, 2000, and culminating in the reforms brought about by the Bhartiya Sakshya Adhiniyam, 2023. The paper examines the concept and meaning of electronic evidence by analysing internationally recognised definitions alongside the Indian statutory framework, and highlights the conceptual distinctions between traditional and electronic evidence. It further explores the distinctive characteristics of electronic evidence—including its volatility, invisibility, susceptibility to manipulation, and capacity for lossless replication—and discusses the challenges these attributes pose for the principles of relevancy, admissibility, hearsay, and best evidence. The paper also addresses critical technical concepts underpinning electronic evidence, such as authentication, chain of custody, hash values, and metadata, and evaluates their legal significance in Indian courts through landmark judicial pronouncements. The analysis reveals that while India has made substantial legislative and judicial progress in recognising and regulating electronic evidence, persistent challenges relating to technical infrastructure, jurisdictional complexities, and the rapid pace of technological change demand continuous adaptation of evidentiary standards.

Keywords: *Electronic Evidence, Indian Evidence Act, Bhartiya Sakshya Adhiniyam, Information*

Technology Act, Digital Forensics, Admissibility, Section 65B, Chain of Custody, Hash Value, Metadata

1. Introduction

The objective of any trial, whether civil or criminal, is the discovery of truth behind disputed facts. The law of evidence governs the means and manner in which litigants can lawfully introduce evidence and prove or disprove the existence or non-existence of a relevant fact. Trial courts accomplish this exercise by presenting and examining both oral and documentary evidence. In civil trials particularly, documentary evidence is considered to have greater evidentiary value than oral evidence, and accordingly, under the Indian Evidence Act, 1872[1] (hereinafter IEA), and the Bhartiya Sakshya Adhiniyam, 2023[2] (hereinafter BSA), provisions have been made for the exclusion of oral evidence by documentary evidence.[3]

In modern times, where computers, artificial intelligence, and the Internet of Things have permeated virtually every facet of life, the field of law is no exception. Courts must increasingly rely on documents available digitally rather than in conventional physical form. A significant proportion of the evidence now offered in trial courts consists of digital documents. Electronic recordings have consequently become a significant part of the trial process, necessitating a deeper understanding of their relevance, admissibility, mode of proof, and probative value within the framework of evidentiary law.

Electronic data—information stored or transmitted in binary form—encompasses emails, CCTV camera recordings, social media content, and numerous other digital artefacts. When parties seek to use such electronic data to prove their case in legal proceedings, these records must satisfy the twin tests of relevancy and admissibility. However, electronic records present their own challenges of authenticity, reliability, and manner of proof that distinguish them from conventional documentary evidence. A physical document can be assessed by the naked human eye, and an experienced judge or lawyer can often form an opinion about its genuineness through physical examination alone. With electronic records, however, there is hardly any tool that a layperson can employ to determine whether the electronic copy produced is the original or not. These intrinsic differences necessitate a re-evaluation of conventional evidentiary rules to accommodate the peculiarities and complexities introduced by digital formats.

2. TRADITIONAL JURISPRUDENCE OF EVIDENCE LAW UNDER THE INDIAN EVIDENCE ACT, 1872

2.1 The Paper-Based Documentary Evidence Framework

The Indian Evidence Act of 1872, established during the British colonial era, has served as a comprehensive statute of evidence law regulating Indian jurisprudence for more than 150 years. Coming into force on 1st September 1872, it marked a historic moment in the legal development of the subcontinent.[4] The Act created a detailed framework categorising evidence into three main divisions: Part I addresses the relevance of facts (Sections 1–55), Part II pertains to proof (Sections 56–100), and Part III discusses the presentation and impact of evidence (Sections 101–167).[5]

The framers of the IEA could not have foreseen the technical progress of the modern digital age. However, the exceptional foresight embedded in the drafting of the Act has enabled courts to adapt and stretch traditional definitions to encompass novel forms of evidence, including electronic records. Section 3 of the Act originally defined "document" as any form of expression upon any substance by any means with the intention of using or recording that matter.[6] Documents produced for the inspection of the court were defined as documentary evidence.[7] Consequently, the IEA relied exclusively on a traditional definition of documentary evidence grounded in paper records and physical documents.[8]

The Act's approach was premised on the concept of "best evidence," requiring the production of original documents, with secondary evidence being admissible only under exceptional circumstances. Section 64 established the fundamental principle that documents must be proved by primary evidence.[9] The traditional framework differentiated between primary evidence—defined as the document itself produced for court inspection[10]—and secondary evidence, which includes certified copies and copies made from the original by mechanical processes.[11] Section 91 further reinforced the primacy of documentary evidence through the "best evidence rule," prohibiting oral evidence to substantiate the contents of documents.

This document-centric methodology sufficiently served the court system during the colonial era and the initial decades of independence. The tangible characteristics of documents offered intrinsic protections against tampering, as modifications to paper documents generally left visible evidence detectable through meticulous scrutiny.

2.2 Relevancy and Admissibility: Foundational Concepts

Under the evidence law, evidence can be given only of facts in issue or to prove the existence or non-existence of every fact declared relevant in Sections 5–55 of the IEA.[12] The same principle has been retained in Section 3 of the BSA.[13] Although neither Act explicitly defines "relevant facts," both provide that evidence can be given only for facts in issue or relevant facts and no other. Justice Mahmood emphasised this principle in *Queen v. Abdullah*[14], noting that the Evidence Act effectively prohibits the employment of any evidence not specifically authorised by the Act itself. Admissibility, by contrast, concerns itself with whether relevant facts are eligible for consideration by the court. As the Supreme Court observed in *State of UP v. Raj Narain*,[15] evidence is admissible and should be received unless there is a legal reason for its rejection; admissibility presupposes relevancy and also denotes the absence of any applicable rule of exclusion. A fact can be relevant yet remain legally inadmissible—for example, privileged spousal communications or confessions made to police officers. Therefore, while every piece of admissible evidence must be relevant, not all relevant evidence is necessarily admissible. Relevancy constitutes a broader category, with admissibility being a narrower subset governed strictly by statutory requirements and judicial interpretations.

2.3 Admissibility and Mode of Proof

A crucial distinction must be drawn between the admissibility of a fact as evidence and the admissibility of the particular manner in which that fact is proved. The courts in trials must undertake a dual inquiry: first, whether the material proffered is admissible, and second, whether it has been proved in the manner the law requires. Ordinarily, the choice of mode of proving a fact is left to the discretion of the party. However, in certain cases the evidence law designates a specific mode of proof that becomes exclusive and mandatory. Electronic records provide a clear illustration: Section 65B of the IEA prescribes the sole procedure for authenticating such data, so parties can satisfy the burden of proof only through strict compliance with that provision.

2.4 Early Judicial Encounters with Digital Evidence

With technological advancements in the later part of the twentieth century, Indian courts began encountering forms of electronic evidence well before the formal legislative amendments of 2000. The earliest instances involved tape recordings, which posed novel questions about admissibility and reliability.[16]

The landmark case of *Yusufalli Esmail Nagree v. State of Maharashtra*[17] in 1968 marked a significant departure from traditional evidence concepts. The three-judge bench of the Supreme Court, dealing with tape-recorded evidence for the first time, held that tape recordings could be admitted as part of *res gestae* under Section 8 of the IEA, provided the time, location, and correctness of the recording were proven by a competent witness and the voices were correctly identified.

Subsequently, in *R.M. Malkani v. State of Maharashtra*,[18] the Supreme Court held that tape-recorded conversations would be admissible provided three conditions were fulfilled: the conversation must be relevant, the voices must be identifiable, and the accuracy must be proved by eliminating the possibility of tampering. The case of *Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdas Mehta*[19] proved particularly significant, as the Apex Court explicitly held that tape recordings were "documents" within the meaning of Section 3 of the IEA—the first judicial interpretation to expand the ambit of documentary evidence beyond its original paper-based conception.

In *Ram Singh & Others v. Col. Ram Singh*,[20] a three-judge bench of the Supreme Court laid down detailed guidelines for the admissibility of tape-recorded conversations, including requirements for voice identification, audibility, accuracy, elimination of tampering, relevance, and safe custody of the recorded cassette. Through these judicial interpretations, tape-recorded conversations were included within the ambit of secondary evidence and admitted by trial courts just like physical documents.

3. The Information Technology Act, 2000: A Watershed Moment

3.1 UNCITRAL Model Law as Foundation

The enactment of the Information Technology Act, 2000[21] represented a watershed moment in the evolution of the Indian legal framework, marking the country's definitive entry into the digital age through comprehensive legislative intervention. The UNCITRAL Model Law on Electronic Commerce, enacted in 1996, provided the conceptual and structural foundation for India's approach.[22] The Model Law was the first extensive global initiative to harmonise the legal frameworks of multiple states with electronic commerce and electronic evidence, establishing that consumers of both paper and electronic communication should receive equivalent legal

protection.[23]

The Model Law established several fundamental principles integrated into Indian legislation. The functional equivalent principle guaranteed that electronic documents would have the same legal validity as their paper-based counterparts, provided they served the same function. The non-discrimination principle asserted that electronic transactions must not be regarded less favourably simply because of their electronic nature. Article 9(1) dealt specifically with the admissibility and evidentiary weight of data messages, providing that rules of evidence should not exclude data messages solely because they were in electronic format or were not in their original form. [24]

3.2 Objectives and Scope of the IT Act

The legislative aim behind the IT Act was clearly focused on enabling e-commerce through substantial emphasis on the admissibility and authentication of electronic records. [25] The Act introduced significant amendments to the IEA to provide appropriate procedures for the production of evidence in electronic form. The comprehensive scope of the Act was reflected in its consequential amendments to four significant pieces of Indian legislation: the Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Banker's Book Evidence Act of 1891, and the Reserve Bank of India Act of 1934.[26] These amendments demonstrated the recognition that electronic evidence required integrated changes across multiple areas of law rather than isolated modifications to individual statutes.

The primary objectives of the IT Act included: providing legal recognition to transactions conducted via electronic data exchange and e-commerce; granting legal recognition to digital signatures for authentication; facilitating electronic filing of documents with government agencies; enabling electronic data storage; providing legal sanction for electronic funds transfers; and recognising electronic books of accounts maintained by bankers.[27]

3.3 Amendments to the Indian Evidence Act

The IT Act fundamentally altered the evidentiary framework through extensive amendments to the IEA. The amendment to Section 3 granted parity to electronic records with traditional paper-based documents for evidentiary purposes.[28] The definition of "admission" in Section 17 was broadened to encompass statements in oral, documentary, or electronic formats, while Section 22A was inserted to permit the relevance of oral evidence concerning the contents of electronic records.

The incorporation of Sections 65A and 65B constituted a significant reform, establishing a defined procedural framework for presenting evidence related to electronic documents. Section 65A stipulated that the contents of electronic records may be substantiated in accordance with Section 65B, which delineated specific criteria for the admissibility of electronic evidence as secondary evidence in the form of computer output. The obligatory nature of Section 65B certification requirements, as determined by pivotal Supreme Court rulings in *Anvar P.V. v. P.K. Basheer*[29] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*,[30] has generated both procedural clarity and practical difficulties in the acceptance of electronic evidence.

4. Concept and Meaning of Electronic Evidence

4.1 International Definitions

One of the earliest and most influential definitions was proposed by the Federal Bureau of Investigation (FBI) in 1998, which defined digital evidence as any information of probative value that is stored or transmitted in digital form.[31] This established the essential idea that electronic evidence must possess probative value while being in a digital format. The International Organisation of Computer Evidence (IOCE) enhanced this by formulating a more precise working definition in 2000, characterising electronic evidence as any information stored or transmitted in binary form that may be relied upon in court.[32]

The Council of Europe adopted a device-centric perspective, defining electronic evidence as any evidence derived from data kept in or generated by devices reliant on software, or data communicated via a computer system or network. Eoghan Casey proposed a tri-partite paradigm, identifying three fundamental components: binary data, a storage device, and software to read and interpret the binary data.[33] Stephen Mason and Daniel Seng offered a systems-oriented definition, characterising electronic evidence as evidence derived from data contained in or produced by any device dependent on a software program, or from data stored on or communicated over a computer system or network.[34]

Burkhard Schafer and Stephen Mason proposed a three-element analytical framework.[35] The first element—Data—encompasses any evidence generated, modified, or stored on a computer. The second element—Device—includes all devices used for data transmission or storage, from traditional computers to mobile phones, smart cards, and navigation systems. The third element—Relevance—restricts electronic evidence to information pertinent to the adjudicative process,

emphasising that not all digital information qualifies as evidence. This comprehensive three-element framework provides a robust analytical tool for understanding electronic evidence across jurisdictions.

4.2 Definition under the Indian Legal Framework

Under Indian jurisprudence, the term evidence has been defined under Section 3 of the IEA to include statements permitted by the court as oral evidence and documents, including electronic records produced for court inspection, as documentary evidence.[36] The Information Technology Act, 2000, establishes the essential framework, with Section 2(1)(t) defining "electronic record" as data, records, images, or sounds that are stored, received, or transmitted in electronic format, including microfilm or computer-generated microfiche.[37]

The complementary definition of "electronic form" under the IT Act refers to any data generated, communicated, received, or stored in media including magnetic, optical, computer memory, microfilm, or similar devices.[38] This technology-neutral perspective anticipates future technological advancements through the comprehensive term "similar device." Furthermore, the Explanation to Section 79A of the IT Act defines electronic evidence as any information of probative value that is stored or transmitted electronically, encompassing computer evidence, digital audio, digital video, mobile phones, and digital fax machines.[39]

The Bhartiya Sakshya Adhiniyam, 2023, further expanded the definitional scope by including statements given electronically under the ambit of oral evidence and introducing the term "digital records" in addition to electronic records in documentary evidence.[40] This legislative update reflects the evolving landscape of information technology and its continuing impact on legal jurisprudence. The importance of electronic evidence was underscored by the Supreme Court in *Tomaso Bruno v. State of Uttar Pradesh*,[41] where the Court observed that the increasing impact of technology in everyday life has made the production of electronic evidence relevant to establish guilt or liability.

5. Conceptual Distinctions and Characteristics of Electronic Evidence

5.1 Distinction from Traditional Evidence

Traditional hard copy evidence is profoundly distinguished from electronic evidence by a variety of factors extending beyond mere format or storage medium. The primary distinction is that

electronic evidence is intrinsically linked to the storage medium, establishing an unbreakable connection between the information and the technological infrastructure necessary to access, interpret, and present it.[42] Unlike a filing cabinet, where documents maintain an independent physical existence and can be examined without specialised equipment, electronic evidence necessitates appropriate hardware, software, and technical expertise to convert the information into a human-readable format.

This technological dependence means that electronic evidence inherently includes not only the substantive information content but also metadata, system logs, and other technical data relevant to understanding the context, authenticity, and integrity of the primary information. This establishes a multi-layered evidentiary framework in which the technical infrastructure itself constitutes evidence, requiring legal professionals to comprehend not only substantive content but also the technological processes that generated, stored, and transmitted it.[43]

5.2 Characteristics of Electronic Evidence

Electronic evidence possesses several distinctive characteristics that differentiate it from conventional forms of proof. First, it is **invisible to the untrained eye**, often existing in digital storage media, volatile memory, network logs, or encrypted formats that are imperceptible to laypersons and require expert intervention for identification, extraction, and analysis.

Second, electronic evidence is **highly volatile**. Data stored in volatile memory, such as RAM, is particularly susceptible to being overwritten through routine device functions, power interruptions, or system operations. Environmental factors such as excessive heat, moisture, or electromagnetic fields can further compromise its stability.

Third, electronic evidence is **subject to damage or loss through regular use**. Routine system processes often alter stored data, and activities such as document saving, file copying, or data transferring across devices consistently modify memory contents, increasing the likelihood of losing or corrupting critical evidence.

Fourth, electronic evidence **can be replicated without deterioration**. Each digital duplicate is an identical reproduction of the original, challenging conventional definitions of "original" evidence. As Mason argues, with paper documents there exists a distinct comprehension between the original and its replicas, as modifications inevitably leave physical evidence. In the digital realm, however, copies and originals are indistinguishable.[44]

Fifth, electronic evidence has a **wider scope**, spanning emails, multimedia files, metadata, internet histories, GPS data, and social media communications. Finally, it **touches interconnected justice issues** beyond typical evidence collection, surpassing conventional jurisdictional and procedural limits and necessitating collaboration among various organisations, jurisdictions, and technological fields.[45]

6. Electronic Evidence and the Rules of Hearsay and Best Evidence

Hearsay evidence is deemed weak because it does not allow the court to scrutinise or cross - examine the original declarant. While the terms "hearsay evidence" are not employed in the IEA or BSA due to their imprecision, the concept is embodied in the requirement that oral evidence must be direct. Under Indian law, hearsay evidence is generally inadmissible,[46] subject to recognised exceptions including *res gestae* (Section 6), admissions and confessions, dying declarations, evidence in former proceedings, and expert opinions.[47]

Electronic evidence presents unique challenges to traditional hearsay analysis. Unlike traditional documents where authenticity can be verified through examination of the author or a witness familiar with the handwriting, electronic records depend entirely on the correctness of the computer system. This creates a fundamental problem: it is practically impossible to demonstrate the "correctness of the system" in every individual case.

The rule of best evidence—requiring production of the best available evidence before the court—is contained in Section 60 of the IEA for oral evidence and Section 64 for documentary evidence, requiring proof by primary evidence. Electronic evidence constitutes an exception to this principle.

It is generally acknowledged that producing the original electronic record consistently is challenging; however, the requirement for the original is waived under Section 65B of the IEA, provided the statutory conditions are met.[48]

7. Challenges with Electronic Evidence

Electronic evidence presents unprecedented complications that fundamentally distinguish digital proof from conventional evidence. These challenges manifest at every stage of the investigative and judicial process and encompass technical, legal, procedural, and practical dimensions.

The **fundamental complexity** of digital data arises from its constantly changing and interrelated nature. Data on hard drive platters consists of information stacked and mixed together over time, creating archaeological layers difficult to separate without advanced technology. Only a small percentage of this vast combination may be pertinent to any given legal issue, and technical data must be painstakingly extracted and translated into forms comprehensible to legal practitioners.

The **fragility and volatility** of electronic evidence—its vulnerability to alteration, damage, and destruction—creates crucial "chain of custody" requirements demanding thorough corroborating documentation throughout the inquiry process.[49] The **circumstantial nature** of most electronic evidence makes it very challenging to link computer activity to particular individuals with the necessary legal certainty. Password protection offers only limited attribution certainty given the potential for sharing, theft, or compromise.

Electronic evidence's unparalleled **susceptibility to manipulation** distinguishes it from physical evidence. Electronic records can be produced, copied, changed, destroyed, and transferred without leaving visible evidence of alteration, raising major concerns about authenticity. The **dynamic nature** of digital information in ever-evolving technology contexts requires legal systems to continuously modify their evidence handling protocols.[50]

The fundamentally global character of electronic evidence presents significant **jurisdictional challenges**, as servers and infrastructure are often situated outside the geographical authority of investigating agencies, necessitating intricate international collaboration. Furthermore, end-to-end encryption restricts access for law enforcement agencies. The rapid growth of **emerging technologies**, particularly artificial intelligence and deepfakes, poses persistent obstacles requiring dynamic authentication procedures. Finally, **technical infrastructure inadequacies** in many courts and forensic labs—including shortages of equipment, training,

and procedural frameworks—further complicate the handling of electronic evidence.

8. Technical Concepts Underpinning Electronic Evidence

8.1 Authentication

Authentication involves confirmation that the evidence recovered is identical to the data originally seized. However, this is not always straightforward. RAM contents perpetually evolve in a functioning computer, making the captured memory contents merely a momentary snapshot with no original for comparison. Once network traffic has been captured, the original data is unavailable and only copies remain. Authentication is a two-step legal procedure involving an initial examination to verify that evidence is as claimed by its proponent, followed by a more detailed analysis to ascertain its probative value. In the initial phase, it may suffice for the individual who collected the evidence to attest to its authenticity; a system administrator, for instance, may testify that the log files presented were generated by their system.

8.2 Chain of Custody

A chain of custody implies continuous, documented accountability for evidence from the moment of collection through every stage of investigation and subsequent processing.[51] Every individual who handles the item must be specifically recorded, preserving an unbroken record that safeguards the evidence's integrity against allegations of tampering or contamination. The chain encompasses five fundamental stages: acquisition, preservation, analysis, copying for court and parties, and presentation in evidence.[52]

The Supreme Court has repeatedly emphasised the importance of maintaining the chain of custody. In *Rahul v. State of Delhi*,[53] the Court stressed that if evidence is not properly documented, collected, packaged, and preserved, it will not meet the legal and scientific requirements for admissibility. In *Manoj v. State of Madhya Pradesh*,[54] the Court refused to rely on DNA evidence where the genuineness of its recovery was suspected.

The Kerala High Court in *Vijesh v. State of Kerala*[55] deprecated the manner in which an investigating officer had handled mobile phone evidence, emphasising that the officer should have ensured a clear link between the hardware and the digital evidence copied from it, and should have maintained a record showing the chain of custody addressing who collected the evidence, how it was collected, who took possession, how it was stored, and the protection offered whilst in storage.

8.3 Hash Values

A hash function is a mathematical technique that processes an input of arbitrary size and produces a fixed-size byte string, termed a "hash value," functioning as a unique "digital fingerprint" of the input data.[56] Hash functions possess several critical characteristics making them invaluable in digital forensics: they generate fixed-length output irrespective of input size; they are deterministic, consistently producing the same hash value for identical inputs; they are computationally irreversible one-way functions; and they possess collision resistance, making the probability of two different inputs producing identical hash values extremely low.

Neither the IEA nor the BSA's operative provisions make express reference to hash values. However, the schedule annexed to the BSA, which prescribes the statutory certificate under Section 63(4) for admissibility of electronic records, includes a designated column requiring specification of the hash value of the digital exhibit. By mandating this cryptographic identifier, the legislature has expressly recognised the hash value as a forensic safeguard authenticating data and securing an unbroken chain of custody.

The Supreme Court in *Ram Kishan Fauji v. State of Haryana*[57] emphasised that hash values authenticate digital evidence by comparing the hash value of evidence with its source, holding that if a CD fails to verify its authenticity through hash value comparison, the transcript derived from it holds no significance. The Delhi High Court in *Sidharth Jaitly v. State*[58] noted that while hash values are not mandatory for voice recording authentication, they serve as additional parameters to verify whether audio or data files are identical.

8.4 Metadata

Metadata—essentially "data about data"[59]—functions as a comprehensive information system offering vital knowledge about electronic records. Each electronic document contains concealed information comprising metadata, defined as data pertaining to document creation and modification, or data generated by the operating system or application concerning a file.[60] Metadata is typically not visible and requires sophisticated software for access or examination. The evidentiary significance of metadata extends beyond mere data description. It discloses extensive details regarding digital images, including location data, camera quality, and lens characteristics. Consumer behaviours can be monitored through metadata as individuals navigate websites, and social media accounts produce substantial metadata useful for anticipating behaviour trends.

Metadata is comprehensively classified into several types: descriptive metadata (titles,

keywords, abstracts); administrative metadata (file type, creator identification, creation date, access permissions); structural metadata (organisational framework and hierarchical structure); technical metadata (format specifications, file size, encoding methods); preservation metadata (long -term preservation documentation); and usage metadata (access patterns, views, downloads, modifications). Each type serves a distinct function in digital forensic investigations and contributes to the holistic understanding of electronic evidence.

8.5 The Section 65B Framework: Procedural Gateway to Admissibility

Section 65B of the Indian Evidence Act represents the cornerstone of the procedural framework governing the admissibility of electronic evidence in India. Inserted by the Information Technology Act, 2000, this provision establishes that any information contained in an electronic record which is printed on paper, stored, recorded, or copied in optical or magnetic media produced by a computer shall be deemed to be a document, provided the conditions stipulated therein are satisfied. The section operates as a self-contained code for the admissibility of electronic records, creating a mandatory procedural pathway that parties must follow when seeking to introduce electronic evidence in legal proceedings.

The conditions prescribed under Section 65B(2) require that the computer output must have been produced by a computer during the period over which it was used regularly to store or process information for the purposes of any activities regularly carried on by a person having lawful control over the computer. The information must have been regularly supplied to the computer in the ordinary course of those activities, and the computer must have been operating properly during the material period. Furthermore, Section 65B(4) mandates the production of a certificate identifying the electronic record, describing the manner of its production, and certifying that the conditions set forth in Section 65B(2) have been satisfied. This certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities.

The judicial interpretation of Section 65B has undergone significant evolution. In the early period following the 2000 amendments, courts adopted varying approaches to the mandatory or directory nature of the certification requirement. The Supreme Court's landmark decision in *Anvar P.V. v.*

P.K. Basheer in 2014 conclusively settled this debate by holding that the requirements of Section 65B are mandatory and that electronic evidence not accompanied by the prescribed certificate is inadmissible. This ruling overruled the earlier position taken in certain decisions

that had treated the certification requirement as merely procedural. The Court clarified that Sections 65A and 65B constitute a complete code governing the admissibility of electronic evidence, and that the general provisions relating to secondary evidence under Sections 63 and 65 of the IEA do not apply to electronic records.

Subsequently, in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* in 2020, the Supreme Court reaffirmed the mandatory nature of Section 65B certification while introducing a pragmatic exception: where the person producing the electronic record is also the owner or controller of the device on which the original information is stored, and the original device is produced before the court, the requirement for a certificate may be relaxed. This nuanced approach reflects the Court's recognition that an overly rigid application of procedural requirements should not defeat the ends of justice, particularly when the authenticity and integrity of the electronic evidence can be independently verified.

9. Conclusion

The concept and interpretation of electronic evidence within the Indian legal framework signify a transformative shift from conventional documentary proof to embracing the complexities of the digital era. Electronic evidence—understood as information stored, received, or transmitted in electronic form—has attained formal legal recognition through extensive amendments to the Indian Evidence Act, 1872, notably introduced by the Information Technology Act, 2000, and now further refined through the Bhartiya Sakshya Adhiniyam, 2023.

The evolution traced in this paper demonstrates a clear trajectory from judicial improvisation to legislative systematisation. The early judicial encounters with tape-recorded evidence in the 1960s and 1970s showcased the Indian judiciary's remarkable flexibility in stretching traditional evidentiary concepts to accommodate technological developments. The decisions in *Yusufalli Esmail Nagree*, *R.M. Malkani*, and *Ziyauddin Burhanuddin Bukhari* collectively laid the jurisprudential foundation upon which subsequent legislative reforms were built. These cases established important precedents regarding voice identification, elimination of tampering, and the classification of recorded conversations as "documents" within the meaning of the evidence law.

The Information Technology Act, 2000, transformed this piecemeal judicial approach into a comprehensive legislative framework. By aligning India's approach with the UNCITRAL Model Law on Electronic Commerce and introducing dedicated provisions for the admissibility and authentication of electronic records, the Act ensured that the Indian legal system was

equipped to handle the evidentiary demands of the digital age. The Section 65B framework, as interpreted through the landmark decisions in *Anvar P.V.* and *Arjun Panditrao Khotkar*, has established clear procedural standards while retaining sufficient flexibility to prevent procedural technicalities from defeating substantive justice.

The unique attributes of electronic evidence—its inherent volatility, vast volume, ease of duplication, dependence on complex hardware and software environments, and susceptibility to damage—demand meticulous handling protocols and a robust legal infrastructure. The technical concepts of authentication, chain of custody, hash values, and metadata have emerged as indispensable pillars of the electronic evidence framework, providing the scientific basis for ensuring the integrity and reliability of digital proof. Their growing recognition in Indian judicial pronouncements—from the Supreme Court's emphasis on hash value verification in *Ram Kishan Fauji* to the Kerala High Court's detailed chain of custody requirements in *Vijesh*—reflects a maturing judicial understanding of digital forensics.

Nevertheless, persistent challenges remain. The rapid pace of technological change—particularly the emergence of artificial intelligence, deepfakes, blockchain technologies, and cloud computing—demands continuous adaptation of evidentiary standards. Jurisdictional complexities arising from the borderless nature of cyberspace, technical infrastructure inadequacies in courts and forensic laboratories, and the absence of transnational competency standards for digital forensics experts all require concerted attention. The Bhartiya Sakshya Adhiniyam, 2023, represents the most recent legislative effort to address these challenges, introducing the concept of "digital records" and expanding the scope of oral evidence to include statements given electronically. However, legislation alone is insufficient; comprehensive capacity-building for judges, lawyers, and investigating agencies, investment in forensic infrastructure, and international cooperation mechanisms are equally essential.

In an era where digital technology permeates all facets of life, electronic evidence has become indispensable in both civil and criminal trials. It compels legal professionals, investigators, and judiciary members to continuously update their understanding and methodologies to manage the intricate nature of digital proof effectively. Despite these complexities, the Indian legal system's commitment to upholding foundational evidentiary principles—authenticity, integrity, and reliability—provides a robust foundation for ensuring that electronic evidence contributes meaningfully to the pursuit of justice in the digital age. The journey from tape recorders to blockchain and artificial intelligence is far from complete, but the legislative and judicial framework that India has constructed offers a solid platform for meeting the evidentiary

challenges that lie ahead.

Endnotes

1. Indian Evidence Act, 1872 (Act No. 1 of 1872).
2. Bhartiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).
3. Sec. 91 to 100 IEA and Sec. 94 to 103 BSA.
4. V. Nageswara Rao, The Indian Evidence Act 18 (LexisNexis, Nagpur 3rd edn., 2019).
5. Indian Evidence Act, 1872.
6. IEA, s. 3 – Definition of "Document."
7. IEA, s. 3 – Definition of "Evidence."
8. Yuvraj Singhal & Ananya Jain, "The Scepticism about 'Electronic Evidence' in India", The Daily Guardian, September 21, 2021.
9. IEA, s. 64.
10. IEA, s. 62.
11. IEA, s. 63.
12. IEA, s. 5.
13. BSA, s. 3.
14. Queen v. Abdullah (1885) ILR 7 All 385.
15. State of UP v. Raj Narain, 1975 AIR 865.
16. Ratanlal Ranchhoddas & Dhirajlal Keshavlal Thakore, The Law of Evidence 1 (LexisNexis Butterworths Wadhwa, 26th edn., 2017).
17. Yusufalli Esmail Nagree v. State of Maharashtra, AIR 1968 SC 147.
18. R.M. Malkani v. State of Maharashtra, [1973] 2 SCR 417.
19. Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdas Mehta, (1976) 2 SCC 17.
20. Ram Singh & Others v. Col. Ram Singh, [1985] Supp. 2 SCR 399.
21. The Information Technology Act, 2000 (Act 21 of 2000).
22. Nikhil Naren, "Two Decades of the Information Technology Act, 2000: Way Forward", The Daily Guardian, September 30, 2020.
23. Talat Fatima, Cyber Crimes pg. 458 (Eastern Book Company, 1st edn., 2011).
24. UNCITRAL Model Law on Electronic Commerce 1996, arts. 5 and 9.
25. N.S. Nappinai, Technology Laws Decoded 45 (LexisNexis, 1st edn., 2017).
26. The Information Technology Act, 2000, Second Schedule.
27. The Information Technology Act, 2000, Statement of Objects and Reasons.

28. Indian Evidence Act, 1872, Section 3, amended by Act 21 of 2000.
29. Anvar P.V. v. P.K. Basheer, [2014] 11 S.C.R. 399.
30. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020 INSC 453.
31. Maria Angela Biasiotti et al., Handling and Exchanging Electronic Evidence Across Europe 174 (Springer International Publishing, 2018).
32. International Organisation on Computer Evidence, G8 Proposed Principles for the Procedures Relating to Digital Evidence (IOCE 2000).
33. E. Casey, Digital Forensics and Investigation (Academic Press, Amsterdam, 1st edn., 2021).
34. S. Mason and D. Seng, Electronic Evidence (The Institute of Advanced Legal Studies, University of London, 4th edn., 2017).
35. B. Schafer & S. Mason, "The Characteristics of Electronic Evidence in Digital Format" in S. Mason (Ed.), Electronic Evidence 23–70 (LexisNexis, 2012).
36. IEA, s. 3.
37. The Information Technology Act, 2000, s. 2(1)(t).
38. The Information Technology Act, 2000, s. 2(1)(r).
39. The Information Technology Act, 2000, s. 79A, Explanation.
40. BSA, s. 2(1)(e).
41. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
42. Allison Stanfield, "Electronic Documents as Evidence: An Issue for All In-house Counsel to Consider" 5(18) International In-house Counsel Journal 3 (2012).
43. Ibid.
44. S. Mason, Electronic Evidence (LexisNexis Butterworths, 3rd edn., 2012).
45. B. Schafer & S. Mason, supra note 35.
46. Anil Maheshwari v. CBI, 2013(136) DRJ 249.
47. Javed Alam v. State of Chhattisgarh, (2009) 6 SCC 450.
48. IEA, s. 65B.
49. E. Casey, Digital Forensics and Investigation (Academic Press, Amsterdam, 1st edn., 2021).
50. Neeraj Aarora, "Admissibility of Electronic Evidence: Challenges for Legal Fraternity," available at http://www.neerajaarora.com/.
51. Parvej Khan v. The State of Maharashtra, 2023 BHC 26670.
52. Yuvraj P. Narvankar, Electronic Evidence in Courtroom: A Lawyer's Manual pg.

158 (LexisNexis, 2022).

53. Rahul v. State of Delhi, (2023) 1 SCC 83.
54. Manoj v. State of Madhya Pradesh, (2023) 2 SCC 353.
55. Vijesh v. State of Kerala, 2018 SCC Online Ker 4637.
56. Yuvraj P. Narvankar, supra note 52, pg. 162.
57. Ram Kishan Fauji v. State of Haryana, (2017) 5 SCC 533.
58. Sidharth Jaitly v. State, LNIND 2015 DEL 5103.
59. S. Mason, Electronic Evidence (LexisNexis Butterworths, 3rd edn., 2012).
60. Kelly Friedman, "Electronic Evidence At Trial," 36 Advoc. Q. 215 (2009).