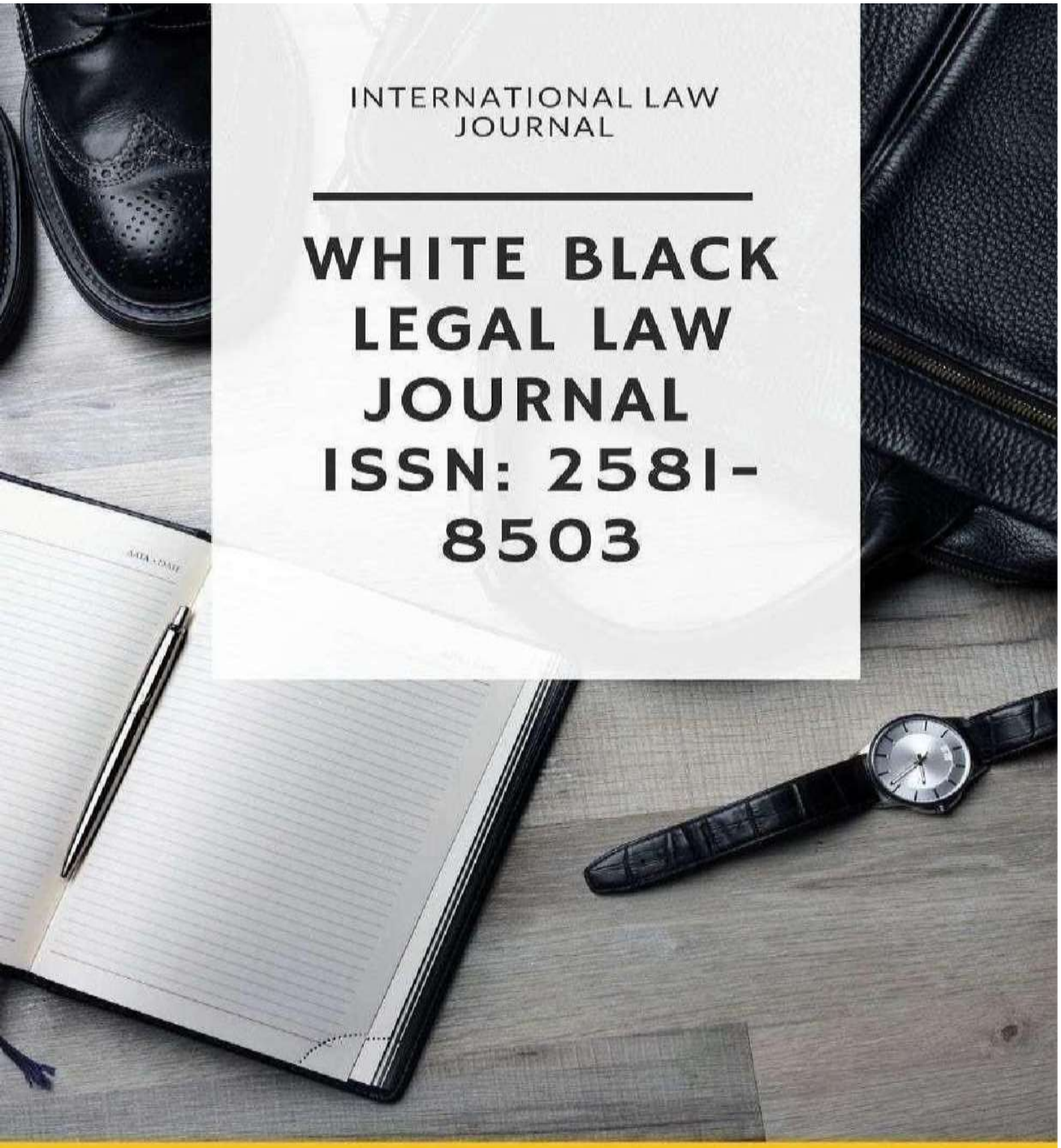

INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 2 | Sep 2025 ISSN: 2581-8503

THE EVIDENTIARY VALUE OF ELECTRONIC RECORDS IN INDIAN COURTS: A LEGAL AND TECHNOLOGICAL ANALYSIS[1]

AUTHORED BY - MUSKAN SHARMA
Ph.D (LAW)
ICFAI UNIVERSITY BADDI, HIMACHAL

Abstract

The rapid advancement of information technology and the increasing reliance on electronic communication and transactions have transformed the evidentiary landscape in Indian courts. The admissibility and evidentiary value of electronic records raise complex questions at the intersection of law and technology. The Information Technology Act, 2000, particularly Section 65A and Section 65B of the Indian Evidence Act, 1872 (as amended), has provided a legal framework for recognizing electronic records as evidence. However, judicial interpretation has oscillated between liberal and strict approaches, resulting in inconsistencies in the treatment of electronic evidence. This research critically examines the statutory provisions, judicial pronouncements, and technological challenges involved in assessing the authenticity, integrity, and reliability of electronic records. It argues that while the law has evolved to accommodate technological realities, significant ambiguities remain, especially in relation to certification under Section 65B, chain of custody, and the application of traditional evidentiary principles to digital formats. By combining a doctrinal legal analysis with an understanding of technological processes, this study aims to highlight gaps, suggest reforms, and propose a balanced approach that safeguards both evidentiary reliability and the right to fair trial.

The exponential growth of digital technologies has transformed the way evidence is created, stored, and presented in courts of law. In India, the admissibility of electronic records is governed primarily by the Indian Evidence Act, 1872, as amended by the Information Technology Act, 2000, with Section 65B standing at the center of judicial debates. Landmark judgments such as "*Anvar P.V. v. P.K. Basheer"* and "*Arjun Panditrao Khotkar v. Kailash*

[1]Authored by Muskan Sharma

Kushanrao Gorantyal" illustrate the judiciary's struggle to balance procedural safeguards with substantive justice in evaluating digital evidence. This paper undertakes a legal and technological analysis of electronic records, examining their evidentiary value, the challenges of authentication, chain of custody, encryption, and emerging technologies. Through a comparative study of foreign jurisdictions and a set of reform-oriented recommendations, the paper argues for a more flexible, technologically robust, and rights-sensitive framework to ensure that electronic evidence serves the cause of justice in India.

Keywords

Electronic Records; Indian Evidence Act, 1872; Information Technology Act, 2000; Section 65B; Admissibility of Evidence; Judicial Interpretation; Digital Authentication; Technological Reliability; Cyber Forensics; Evidentiary Value.

Introduction

The digital age has profoundly altered the way evidence is created, stored, and presented in judicial proceedings. Electronic records, ranging from emails, text messages, CCTV footage, and call data records to blockchain transactions, have become crucial in both civil and criminal cases. The transformation from traditional paper-based evidence to electronic forms has posed significant challenges for Indian courts in terms of authenticity, admissibility, and reliability.[2]

The Indian Evidence Act, 1872 (hereinafter "IEA"), originally enacted in a pre-digital era, was amended through the Information Technology Act, 2000, to incorporate provisions that recognize and regulate the evidentiary use of electronic records.[3] The most debated provisions—Sections 65A and 65B of the IEA—establish conditions under which electronic evidence may be admitted. However, judicial interpretation of these provisions has been inconsistent, oscillating between rigid compliance and pragmatic flexibility.[4]

Cases such as "State (NCT of Delhi) v. Navjot Sandhu"[5] (the Parliament Attack case), Anvar

[2]S. Kalyani, "Evidentiary Challenges in the Digital Era," *Journal of Indian Law and Technology*, Vol. 13, 2017, p. 45.
[3]Information Technology Act, 2000, No. 21 of 2000.
[4]R. Banerjee, "Section 65B and the Admissibility of Electronic Evidence: A Critical Appraisal," *Indian Bar Review*, Vol. 47, 2020, p. 213.
[5]*State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

P.V. v. P.K. Basheer[6], and "Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal"[7] illustrate the evolving judicial stance on the evidentiary value of electronic records. These decisions reveal a judicial struggle to reconcile the imperatives of technological reliability with procedural fairness and evidentiary safeguards.

The central issue remains: how should Indian courts ensure that electronic records, which are vulnerable to tampering, alteration, and manipulation, are treated as reliable evidence without undermining the rights of the accused or the integrity of judicial proceedings? This research addresses that issue by examining the legal framework, judicial interpretations, and technological realities governing electronic records in India.

Research Methodology

This research adopts a doctrinal methodology, relying primarily on the analysis of statutory provisions, judicial decisions, and academic writings on the evidentiary value of electronic records. The doctrinal approach is appropriate because the study focuses on interpreting and critiquing the legal framework governing electronic evidence under the Indian Evidence Act, 1872, as amended by the Information Technology Act, 2000.[8]

Additionally, a comparative approach is employed by examining international practices in jurisdictions such as the United States, the United Kingdom, and Singapore, where courts have evolved mechanisms to ensure reliability and admissibility of electronic records.[9] This comparative dimension allows identification of best practices that may inform reforms in India.

The research also adopts an interdisciplinary perspective, incorporating insights from computer science and cyber forensics to understand the technological processes underlying electronic evidence.[10] This is essential because the legal evaluation of electronic records cannot be divorced from their technological foundations, particularly in matters of authenticity, integrity, and chain of custody.

[6]*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[7]*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[8]M.P. Jain, *Indian Evidence Act*, 19th ed., LexisNexis, 2021, p. 556.
[9]S. Mason and D. Seng (eds.), *Electronic Evidence*, 5th ed., Institute of Advanced Legal Studies, London, 2021, p. 88.
[10]R. Sharma, "Cyber Forensics and the Law of Evidence in India," *NUJS Law Review*, Vol. 11, 2018, p. 143.

The study relies on primary sources such as statutes, amendments, and case law, and secondary sources including journal articles, law commission reports, and expert commentary. The data is qualitative and analytical in nature, rather than empirical, since the primary focus lies on legal interpretation and theoretical frameworks rather than field surveys.[11]

Hypothesis

The central hypothesis of this research is that the Indian legal framework on electronic records, particularly Sections 65A and 65B of the Indian Evidence Act, 1872, though progressive in recognizing digital evidence, remains inadequate in ensuring consistent admissibility and reliability due to procedural rigidity, lack of judicial uniformity, and insufficient technological integration.[12]

It is further hypothesized that judicial inconsistency—ranging from the liberal approach in Navjot Sandhu[13] to the strict compliance mandated in Anvar P.V.[14] and reaffirmed in Arjun Panditrao[15]—has created uncertainty for litigants, law enforcement agencies, and courts. This uncertainty undermines the effective use of electronic records in both civil and criminal trials. Finally, the research hypothesizes that a balanced model, drawing from international best practices and supported by forensic verification mechanisms, can provide a more reliable framework for evaluating electronic records in India, thereby strengthening evidentiary certainty and safeguarding fair trial rights.[16]

Research Questions

In order to test the above hypothesis, this research seeks to address the following key questions:

1. What is the current legal framework governing the admissibility of electronic records in Indian courts, and how have Sections 65A and 65B of the Indian Evidence Act, 1872 been interpreted by the judiciary?
2. How have Indian courts balanced the need for technological reliability of electronic evidence with the principles of natural justice and fair trial?

[11]Law Commission of India, 185th Report on *Amendment to the Indian Evidence Act, 1872*, March 2003, p. 22.
[12]A. Kumar, "Evidentiary Value of Electronic Records: Judicial Trends in India," *Indian Journal of Law and Technology*, Vol. 15, 2019, p. 77.
[13]*State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
[14]*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[15]*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[16]S. Mason, "International Standards for Electronic Evidence," *Computer Law & Security Review*, Vol. 34, 2018, p. 304.

3. What inconsistencies or ambiguities exist in judicial pronouncements on the evidentiary value of electronic records, and what are their implications for litigants and law enforcement agencies?
4. How do other jurisdictions, such as the United States, the United Kingdom, and Singapore, address the admissibility and reliability of electronic records, and what lessons can India derive from them?
5. What reforms—legal, procedural, and technological—are necessary to create a coherent and reliable framework for electronic evidence in India?

Literature Review

Scholarly engagement with electronic evidence in India has largely revolved around the interpretation of Sections 65A and 65B of the Indian Evidence Act, 1872. Early literature acknowledged the pioneering role of the Information Technology Act, 2000, in extending legal recognition to electronic records.[17] However, commentators have repeatedly emphasized that statutory provisions alone are insufficient to address the complexities of digital evidence.[18]

Kalyani argues that the digital era has posed unprecedented challenges to courts, particularly regarding the authenticity and integrity of electronic records.[19] According to her, the inherent vulnerability of electronic evidence to tampering necessitates stringent safeguards and judicial caution. Similarly, Banerjee highlights the "procedural rigidity" of Section 65B certification, observing that while it ensures reliability, it has also created procedural bottlenecks for litigants and investigators.[20]

Judicial pronouncements have been subject to significant academic scrutiny. The Supreme Court's decision in Navjot Sandhu was criticized for diluting the mandatory requirements of Section 65B by allowing oral evidence to prove electronic records.[21] In contrast, the Anvar P.V. judgment was welcomed for restoring the strict requirement of certification, though scholars noted that its rigid stance created practical difficulties in cases involving third-party

[17]A. Kumar, "Recognition of Electronic Evidence under the IT Act, 2000," *Indian Journal of Legal Studies*, Vol. 8, 2003, p. 34.
[18]N. Menon, "Electronic Records and the Law of Evidence in India," *ILI Law Review*, Vol. 55, 2015, p. 122.
[19]S. Kalyani, "Evidentiary Challenges in the Digital Era," *Journal of Indian Law and Technology*, Vol. 13, 2017, p. 45.
[20]R. Banerjee, "Section 65B and the Admissibility of Electronic Evidence: A Critical Appraisal," *Indian Bar Review*, Vol. 47, 2020, p. 213.
[21]*State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

custodians of electronic data.[22] The subsequent clarification in Arjun Panditrao has been studied as an attempt to strike a balance, though opinions remain divided on whether it has resolved or deepened the evidentiary conundrum.[23]

Comparative scholarship provides insights into how other jurisdictions have dealt with similar challenges. Mason and Seng, in their authoritative work Electronic Evidence, underline the importance of establishing international standards for admissibility, including principles of authenticity, chain of custody, and forensic reliability.[24] Tapia's comparative analysis demonstrates that jurisdictions like the United States and the United Kingdom have developed pragmatic approaches, often relying on expert testimony and forensic validation rather than rigid certification requirements.[25]

The literature also emphasizes the interdisciplinary nature of the issue. Sharma notes that legal frameworks must integrate with technological advances, particularly cyber forensics, to ensure that courts can meaningfully evaluate electronic evidence.[26] This interdisciplinary lens underscores the necessity of collaboration between legal practitioners, forensic experts, and technologists in shaping a coherent evidentiary regime.

In summary, the existing literature recognizes the progressive intent behind the Indian statutory framework but critiques its inconsistent judicial application and procedural rigidity. Scholars advocate reforms that blend legal certainty, procedural fairness, and technological sophistication to enhance the evidentiary value of electronic records in India.

The Legal Framework Governing Electronic Records in India

The legal recognition of electronic records in India is the product of statutory reform necessitated by the rise of digital communication and commerce. The **I**ndian Evidence Act, 1872 (IEA), originally enacted in a pre-digital era, was amended by the Information Technology Act, 2000 (IT Act, 2000) to provide a statutory basis for electronic evidence. The

[22]*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[23]*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[24]S. Mason and D. Seng (eds.), *Electronic Evidence*, 5th ed., Institute of Advanced Legal Studies, London, 2021, p. 88.
[25]R. Tapia, *Digital Evidence and Courtroom Practice in Common Law Countries*, Oxford University Press, 2020, p. 132.
[26]R. Sharma, "Cyber Forensics and the Law of Evidence in India," *NUJS Law Review*, Vol. 11, 2018, p. 143.

amendments introduced critical provisions—most notably Sections 65A and 65B of the IEA—which specifically govern the admissibility of electronic records.

Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B. Section 65B lays down the conditions under which information contained in electronic records is deemed admissible as evidence. The provision requires that such information must be produced in the form of a computer output and must be accompanied by a certificate satisfying specific requirements, including the identification of the electronic record, the description of the manner in which it was produced, and particulars of the device used to produce the record. This certificate must be signed by a person occupying a responsible official position in relation to the operation of the device or the management of the relevant activities.

The introduction of these provisions was intended to address two fundamental concerns regarding electronic evidence: authenticity and reliability. Electronic records are inherently more susceptible to alteration, tampering, and manipulation than paper records.[27] The requirement of certification under Section 65B was thus envisaged as a safeguard to ensure that only records which meet technological and procedural standards are admitted in court.

The statutory framework also intersects with other legal provisions. For instance, Section 3 of the IT Act, 2000 provides legal recognition to electronic signatures, while Section 4 grants validity to electronic records, equating them with written documents.[28] The combined effect of these provisions is that electronic records are not merely supplementary to traditional evidence but have become a full-fledged category of admissible evidence within the Indian legal system.

However, despite this seemingly comprehensive framework, ambiguities remain. One major issue is whether compliance with Section 65B is mandatory or directory. Initially, in Navjot Sandhu, the Supreme Court allowed for the admission of electronic evidence even without a certificate, holding that such evidence could also be proved through oral testimony. This interpretation diluted the statutory requirement, prompting criticism from scholars and practitioners. Later, in Anvar P.V., the Court reversed course, holding that certification is

[27]N. Menon, "Electronic Records and the Law of Evidence in India," *ILI Law Review*, Vol. 55, 2015, p. 122.
[28]Sections 3 and 4, Information Technology Act, 2000.

mandatory, thus restoring procedural strictness. Finally, in Arjun Panditrao, the Supreme Court clarified that Section 65B certification is mandatory unless the device itself is produced before the court.

The oscillation between these judicial interpretations has created uncertainty for trial courts, investigators, and litigants. For example, in cases involving third-party custodians such as telecom companies or internet service providers, obtaining a Section 65B certificate can be practically difficult. This creates a tension between the law's demand for procedural compliance and the practical realities of digital evidence collection.

Further, unlike some other jurisdictions, India does not yet have a detailed statutory framework governing chain of custody for electronic evidence. Chain of custody ensures that the electronic record presented in court is the same as the one originally collected and has not been altered in transit.[29] The absence of such statutory clarity often forces courts to rely on general evidentiary principles, leaving significant discretion to judges.

Thus, while the statutory framework under the IT Act, 2000 and the Indian Evidence Act, 1872 has laid a foundational structure for electronic records, its effectiveness has been undermined by judicial inconsistency, procedural rigidity, and technological gaps. Addressing these issues requires not only legislative reform but also a more nuanced understanding of digital technology by the judiciary.

Judicial Interpretation and Evolving Case Law

The interpretation of Sections 65A and 65B of the Indian Evidence Act, 1872 has been one of the most contested issues in Indian jurisprudence. Judicial pronouncements have oscillated between liberal and strict approaches, creating uncertainty in the evidentiary treatment of electronic records. The trajectory of case law reveals a gradual evolution from flexibility to procedural rigidity, followed by partial reconciliation.

The starting point is the landmark judgment in "State (NCT of Delhi) v. Navjot Sandhu (2005)", commonly known as the Parliament Attack case. In this case, the prosecution relied

[29]S. Mason and D. Seng (eds.), *Electronic Evidence*, 5th ed., Institute of Advanced Legal Studies, London, 2021, p. 134.

heavily on electronic evidence, such as call data records (CDRs). The Supreme Court held that even if a certificate under Section 65B was not produced, electronic evidence could still be admitted if it was supported by oral testimony from a competent witness. This interpretation diluted the statutory requirement and allowed electronic records to be proved in the same manner as traditional documentary evidence. While the decision facilitated admissibility, it was criticized for undermining the legislative intent behind Section 65B.

A significant shift occurred with "Anvar P.V. v. P.K. Basheer (2014)". Here, the Court overruled Navjot Sandhu, holding that compliance with Section 65B is mandatory. The Court clarified that electronic records are secondary evidence and can only be admitted upon fulfillment of the conditions in Section 65B. It ruled that oral testimony or other forms of proof cannot substitute for the statutory certificate. The Anvar decision brought much-needed clarity but also created procedural hurdles. For instance, in cases where electronic evidence is in the custody of third parties (e.g., telecom companies or internet service providers), litigants often struggle to obtain the requisite certificate.[30]

This strict approach was reaffirmed in "Shafhi Mohammad v. State of Himachal Pradesh" (2018), where the Supreme Court attempted to dilute Anvar by allowing courts to admit electronic evidence without certification in situations where the party did not have control over the device.[7] However, this judgment led to confusion, as it contradicted the binding precedent of Anvar.

The conflict was finally addressed in "Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal" (2020), a Constitution Bench judgment. The Court reaffirmed that Section 65B certification is mandatory but clarified that it is not required if the original electronic device itself is produced before the court. Further, it observed that in cases where third-party custodians hold the electronic data, litigants may apply to the court for issuance of appropriate directions to secure the certificate. This judgment attempted to strike a balance between procedural strictness and practical feasibility.

Other important cases have also contributed to the jurisprudence. In "Tomaso Bruno v. State

[30]R. Banerjee, "Section 65B and the Admissibility of Electronic Evidence: A Critical Appraisal," *Indian Bar Review*, Vol. 47, 2020, p. 221.

of U.P. (2015)", the Supreme Court emphasized the importance of CCTV footage in criminal trials, observing that modern technologies provide accurate and reliable sources of evidence that courts must embrace. Similarly, in "Kishan Chand v. State of Haryana (2013)", the Court relied on call data records to corroborate witness testimonies, underlining the growing evidentiary significance of electronic records.

Despite these developments, challenges remain. Trial courts often grapple with the procedural complexities of Section 65B. Inconsistencies in High Court rulings further complicate the matter, with some courts adopting a liberal stance and others adhering strictly to statutory compliance.[31] This lack of uniformity undermines predictability and legal certainty, both of which are crucial for the effective functioning of the justice system.

Comparatively, the Indian judiciary's struggle mirrors global trends, where courts worldwide are grappling with the admissibility of electronic records. However, unlike jurisdictions such as the United States or the United Kingdom, Indian jurisprudence has not yet evolved a robust doctrine of judicial discretion that balances statutory compliance with practical considerations.[32]

Thus, the judicial journey from Navjot Sandhu to Arjun Panditrao reflects both the progress and pitfalls of India's approach. While the recognition of electronic records is well established, the insistence on procedural formalism continues to hinder their effective use.

Technological Challenges in Admissibility and Authentication

While the statutory framework under the Indian Evidence Act, 1872 and the Information Technology Act, 2000 recognizes electronic records as admissible evidence, the technological vulnerabilities inherent in digital systems present unique challenges to courts. The evaluation of authenticity, reliability, and integrity of electronic records requires an understanding of both legal principles and technical processes.

[31]P. Satish, "Electronic Evidence and the Indian Evidence Act," *National Law School Journal*, Vol. 12, 2016, p. 94.
[32]S. Mason and D. Seng (eds.), *Electronic Evidence*, 5th ed., Institute of Advanced Legal Studies, London, 2021, p. 142.

Authenticity and Tampering

Unlike traditional paper records, electronic records can be easily altered without leaving visible traces.[33] Metadata (such as time stamps, location data, and device identifiers) can provide some assurance of authenticity, but metadata itself is susceptible to manipulation.[34] In criminal cases, where the liberty of the accused is at stake, the possibility of tampering necessitates stringent safeguards. For instance, in Tomaso Bruno v. State of U.P., the Court stressed the importance of CCTV footage but also acknowledged that its evidentiary value depends on proof of its authenticity.

The Problem of Section 65B Certification

From a technological perspective, Section 65B's certification requirement poses difficulties because the person issuing the certificate must confirm the integrity of the device and the process by which the record was produced. However, in cases where electronic data is stored on third-party servers, such as telecom service providers, cloud storage platforms, or social media companies, litigants often lack access to the technical personnel capable of issuing such certificates. This gap between legal requirements and technological realities leads to evidentiary exclusions that undermine the search for truth.

Chain of Custody and Digital Forensics

The chain of custody is critical in ensuring that electronic evidence presented in court is the same as the evidence originally collected. In practice, however, Indian courts lack a uniform protocol for establishing digital chain of custody.[35] By contrast, jurisdictions such as the United States employ forensic standards such as the Federal Rules of Evidence and guidelines from the National Institute of Standards and Technology (NIST) to ensure integrity. In India, while forensic science laboratories (FSLs) play a role, their limited capacity and lack of standardization often lead to delays and inconsistencies.

Encryption and Data Privacy

With the increasing use of encryption technologies, courts face the challenge of accessing and decrypting electronic records. For example, encrypted communication on platforms such as

[33]R. Sharma, "Cyber Forensics and the Law of Evidence in India," *NUJS Law Review*, Vol. 11, 2018, p. 148.
[34]M. Birnhack, "The Fragility of Metadata as Legal Evidence," *International Journal of Law and Information Technology*, Vol. 27, 2019, p. 71.
[35]N. Menon, "Electronic Records and the Law of Evidence in India," *ILI Law Review*, Vol. 55, 2015, p. 129.

WhatsApp or Signal may contain crucial evidence, but strong end-to-end encryption makes it nearly impossible to retrieve or verify without compromising user privacy.[36]The absence of a clear legal framework balancing evidentiary needs and privacy rights further complicates matters.

Reliability of Emerging Technologies

Courts are increasingly encountering evidence derived from emerging technologies such as blockchain, artificial intelligence, and digital forensics tools. While blockchain records are often considered tamper-resistant due to cryptographic hashing, questions remain about whether courts are equipped to evaluate the reliability of such systems. Similarly, digital forensics tools used to recover deleted files or extract data from devices must themselves be subject to scrutiny for accuracy and reliability. Without judicial familiarity with these technologies, there is a risk of either blind acceptance or undue skepticism.

Lack of Judicial Technical Capacity

Perhaps the most pressing challenge is the judiciary's limited technical expertise. As scholars have noted, judges are trained in law, not computer science, and often struggle to evaluate the technical nuances of electronic evidence. Training programs and specialized forensic units within the judiciary could help bridge this gap, but such initiatives remain sporadic and insufficient in India.

Comparative Perspectives from Other Jurisdictions

The evidentiary value of electronic records has become a global concern, prompting different jurisdictions to adopt diverse approaches balancing legal certainty, technological reliability, and protection of rights. A comparative analysis offers valuable insights for India, where courts continue to grapple with the interpretation of Section 65B and the authentication of digital evidence.

1. United States: Federal Rules of Evidence and Forensic Standards

In the United States, the admissibility of electronic records is governed by the Federal Rules of Evidence (FRE). Rule 901 lays down that evidence must be authenticated by "evidence

[36]A. West, "Encrypted Communications and Evidentiary Challenges," *Harvard Journal of Law & Technology*, Vol. 34, 2021, p. 201.

sufficient to support a finding that the item is what the proponent claims it is." This broad standard gives judge's discretion to admit electronic evidence provided its authenticity is demonstrated through testimony, technical evidence, or forensic certification.

Further, specialized forensic protocols have been developed by institutions such as the National Institute of Standards and Technology (NIST), which issue guidelines on collection, preservation, and analysis of digital evidence.[37] Courts frequently rely on these standards, and expert testimony plays a significant role. Importantly, the U.S. courts have embraced flexibility, avoiding rigid statutory requirements like India's Section 65B certificate, thereby prioritizing substantive justice over technicalities.[38]

2. United Kingdom: Civil Evidence Act and Judicial Guidance

The United Kingdom follows the Civil Evidence Act, 1995, which recognizes electronic records as admissible provided their reliability is established. Courts focus on whether the system producing the evidence was operating properly and whether the record was created in the ordinary course of business. The English judiciary has also issued Practice Directions on Digital Disclosure, ensuring that parties exchange and preserve electronic data in a transparent manner. Unlike India, the UK does not impose mandatory certification requirements but emphasizes reliability through system integrity and chain-of-custody.

3. Singapore: Technology-Neutral Approach

Singapore has been a pioneer in adopting a technology-neutral evidentiary framework. The Evidence Act of Singapore, amended in 2012, expressly provides that electronic records are admissible without distinction from traditional evidence. Courts there place reliance on expert testimony and digital forensics to assess authenticity. Moreover, Singapore's judiciary has actively invested in technological infrastructure, including e-litigation platforms and specialized training for judges, ensuring better preparedness in dealing with complex digital evidence.[39]

[37]National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response*, Special Publication 800-86 (2006).
[38]G. Greenleaf, "Electronic Evidence and the U.S. Courts: Lessons for Asia," *Asian Journal of Comparative Law*, Vol. 9, 2014, p. 201.
[39]T. S. Lim, "Admissibility of Electronic Evidence in Singapore: A Technology-Neutral Approach," *Singapore Academy of Law Journal*, Vol. 29, 2017, p. 341.

4. European Union: eIDAS Regulation

Within the European Union, the eIDAS Regulation (2014) provides uniform standards for electronic identification and trust services, including digital signatures and electronic seals. Courts across EU member states accord presumptive authenticity to qualified electronic signatures and timestamps, thereby reducing disputes over genuineness. This approach reflects a policy of harmonization, ensuring that electronic records enjoy cross-border recognition and reliability.

5. Lessons for India

From these jurisdictions, several lessons emerge for India:

- The **f**lexibility of the U.S. model, which avoids rigid procedural hurdles, suggests that India could consider diluting the strict Section 65B certificate requirement.
- The UK emphasis on system reliability and chain-of-custody protocols highlights the need for standardized forensic procedures in India.
- Singapore demonstrates the importance of judicial training and technology adoption, ensuring courts remain abreast of technological developments.
- The EU's trust-based system of digital signatures and timestamps indicates that India could integrate stronger technological standards, backed by statutory presumptions, to strengthen evidentiary reliability.

Unless India draws from these comparative experiences, it risks allowing procedural rigidity and lack of technical capacity to undermine the probative value of electronic records.

The Way Forward — Reforms and Recommendations for India

A coherent framework for the evidentiary use of electronic records in India must align statutory text, procedural practice, and technological realities. The following reforms are proposed across four axes—legislative, procedural, technological/forensic, and institutional—together with privacy and cross-border considerations.

1. Legislative Reforms

a) **Clarify the status of Section 65B and introduce functional equivalence:** Parliament should amend Section 65B to (i) expressly recognize multiple modes of authentication (including hash-based verification and trusted timestamps) as alternatives to, or substitutes for, the present certificate, and (ii) codify the Arjun Panditrao holding that certification is unnecessary when the original device is produced. This would preserve

reliability while preventing exclusion of probative material due to certificate unavailability from third-party custodians.

b) **Codify chain-of-custody for electronic evidence:** A new Schedule or set of Rules under the Evidence Act should define a statutory chain-of-custody protocol: acquisition via bit-for-bit imaging; mandatory use of write-blockers; SHA-256 (or higher) hashing on acquisition and every transfer; tamper-evident sealing; and auditable logs.

c) **Strengthen presumptions tailored to digital records:** While India already recognizes presumptions for electronic agreements and signatures (IEA Sections 85A, 85B, 85C, 88A, 90A), these should be updated to (i) provide a rebuttable presumption of integrity for records bearing qualified electronic signatures or trusted timestamps compliant with notified standards, and (ii) extend Section 90A's "five-year" presumption to defined categories of business records retained under statutory retention duties.

d) **Embed expert opinion on electronic evidence:** Give teeth to Section 45A (opinion of Examiner of Electronic Evidence) by notifying minimum qualifications, independence safeguards, and timelines for reports, thereby creating a trusted roster of neutral experts accessible to all courts.

2. Procedural Reforms (Court-Facing)

(a) Model Practice Direction on Electronic Evidence: The Supreme Court (or High Courts under Article 227) should promulgate uniform Practice Directions prescribing: (i) a model Section 65B certificate with core fields (device ID, system description, hash values, extraction workflow); (ii) timelines and procedures for compelling third-party custodians (telecom, cloud, platforms) to furnish certificates and raw logs; and (iii) early case management conferences to identify digital sources and preservation duties.

(b) Discovery, disclosure, and preservation: Borrowing from UK Practice Directions on Electronic Disclosure, courts should require parties to exchange Electronic Documents Questionnaires early in proceedings, address formats (native vs. TIFF/PDF), metadata fields, and search methodologies, and issue preservation orders with sanctions for spoliation.

(c) Device-production vs. certified output: Operationalize Arjun Panditrao by prioritizing device production where feasible (e.g., CCTV DVRs, source phones), with court-supervised imaging; where not feasible, accept certified computer outputs with corroborating logs.

3. Technological & Forensic Reforms

(a) National Standards for Digital Evidence: Notify Bureau of Indian Standards (BIS)/MeitY rules harmonized with international benchmarks (e.g., NIST SP-800 series) for acquisition, examination, and reporting, including mobile forensics and cloud artifacts.[40]Standards should specify hashing algorithms, imaging formats (E01/RAW), chain-of-custody forms, and validation/verification reporting.

(b) Capacity-building of FSLs and accreditation: Mandate ISO/IEC 17025 accreditation for digital forensics labs, expand infrastructure, and publish turnaround-time targets. Courts should prefer accredited labs and require disclosure of tool versions, validation studies, and error rates.

(c) Trusted time-stamping and e-seals: Leverage the IT Act trust framework to notify trusted timestamping and electronic seals for businesses and public bodies, creating presumptions of integrity akin to the EU's eIDAS model.

(d) Tool transparency and validation: Require disclosure of forensic toolchains (acquisition software, parsing tools), hash values of images, and method validation (test data, known-answer tests). Courts should be wary of black-box analytics unless independently validated and subject to cross-examination.

(e) Secure evidence management: Adopt court-controlled evidence vaults with role-based access, immutable logging, periodic re-hashing, and reproducible workflows to minimize disputes over manipulation.

4. Institutional & Human-Capital Reforms

(a) Judicial and Bar training: Establish mandatory Continuing Judicial Education modules on digital evidence (hashing, metadata, logs, encryption, cloud artifacts). Partner with technical universities and CERT-In for hands-on labs.

(b) Neutral technical assistance: Constitute Court-Appointed Neutral Experts (CANE) panels under Section 45A to assist trial judges with protocol design (e.g., how to image a DVR), tool validation, and explaining error rates to jurists.

(c) Specialized e-evidence benches or lists: Pilot specialized lists in metropolitan trial courts to handle high-volume digital evidence, improving consistency and speed.

[40]National Institute of Standards and Technology (NIST), **SP 800-101 Rev. 1: Guidelines on Mobile Device Forensics** (2014); **SP 800-86: Guide to Integrating Forensic Techniques into Incident Response** (2006).

5. Privacy, Due Process, and Cross-Border Access

(a) Privacy by design: Align evidentiary practices with Puttaswamy (privacy as a fundamental right) and the Digital Personal Data Protection Act, 2023: narrowly tailored collection orders, minimization, secure handling, and protective orders for sensitive personal data.[41]

(b) Encrypted platforms and compelled production: Issue clear guidance on lawful access to encrypted content and metadata-only production where content is technically unavailable, ensuring proportionality and auditability of requests.

(c) Cross-border evidence: Streamline MLAT and executive cooperation channels; publish a model data request **protocol** for major platforms, mapping Indian legal thresholds to platform transparency procedures; consider alignment with Budapest Convention principles on expedited preservation and disclosure, even pending accession.[42]

6. Putting It Together: A Practical Roadmap for Trial Courts

1. **Early identification & preservation:** Case-management order identifying devices/accounts; immediate preservation letters and imaging.
2. **Standardized certification:** Use the **model 65B certificate** or produce the original device for court-supervised imaging.
3. **Chain-of-custody rigor:** Hash on acquisition and every transfer; maintain sealed evidence with immutable logs.
4. **Transparent forensics:** Accredited labs; disclosed toolchains; validation exhibits; reproducible reports with hash verification.
5. **Rights safeguards:** Minimization; protective orders; privacy-impact notes when sensitive data is processed.
6. **Adjudicative clarity:** Judicial checklists for authenticity (hash match), reliability (tool validation), and fairness (opportunity to test/challenge).

These reforms collectively reduce exclusionary technicalities, enhance reliability, and protect due process, enabling Indian courts to harness digital evidence without compromising fairness.

[41] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; **Digital Personal Data Protection Act, 2023** (Act 22 of 2023).
[42] Council of Europe, **Convention on Cybercrime (Budapest Convention)**, 2001 (principles on expedited preservation and mutual assistance).

Conclusion

The evidentiary value of electronic records in India represents a convergence of law and technology, yet the system remains fraught with inconsistencies. On one hand, statutory recognition under the Indian Evidence Act, 1872, read with the Information Technology Act, 2000, firmly establishes electronic records as admissible. On the other hand, the rigidities of Section 65B certification, the lack of uniform chain-of-custody protocols, and insufficient judicial technical capacity continue to hinder effective adjudication.

Judicial precedents from Anvar P.V. to Arjun Panditrao have attempted to clarify the contours of admissibility, but they also highlight the tension between procedural rigor and substantive justice. Comparative perspectives from the United States, United Kingdom, Singapore, and the European Union demonstrate that flexibility, standardization, and judicial preparedness are critical in addressing these challenges.

For India, the way forward lies in a multi-pronged reform agenda: legislative amendments to modernize Section 65B, procedural innovations such as model practice directions, technological reforms in forensic standards and accreditation, and capacity-building initiatives for judges and lawyers. These reforms must also be harmonized with fundamental rights jurisprudence, especially privacy, and must address the cross-border nature of much digital evidence.

Ultimately, the legitimacy of Indian courts in the digital era will depend on their ability to ensure that electronic records are evaluated not merely on formal compliance but on their authenticity, reliability, and fairness. By bridging the gap between technological reality and legal doctrine, India can transform electronic evidence from a source of uncertainty into a cornerstone of justice.

Bibliography

Books

- Mason, Stephen & Seng, Daniel (eds.), Electronic Evidence, 5th ed., Institute of Advanced Legal Studies, London, 2021.
- Sharma, R., Cyber Forensics and the Law of Evidence in India, Eastern Book Company, Lucknow, 2019.

- Bhansali, S.R., The Indian Evidence Act, 22nd ed., Universal Law Publishing, New Delhi, 2022.

Journal Articles

- Banerjee, R., "Section 65B and the Admissibility of Electronic Evidence: A Critical Appraisal," Indian Bar Review, Vol. 47, 2020, p. 219.
- Birnhack, M., "The Fragility of Metadata as Legal Evidence," International Journal of Law and Information Technology, Vol. 27, 2019, p. 71.
- Kalyani, S., "Judicial Capacity and Digital Evidence," Journal of Indian Law and Technology, Vol. 13, 2017, p. 58.
- Lim, T.S., "Admissibility of Electronic Evidence in Singapore: A Technology-Neutral Approach," Singapore Academy of Law Journal, Vol. 29, 2017, p. 341.
- Greenleaf, G., "Electronic Evidence and the U.S. Courts: Lessons for Asia," Asian Journal of Comparative Law, Vol. 9, 2014, p. 201.
- Menon, N., "Electronic Records and the Law of Evidence in India," ILI Law Review, Vol. 55, 2015, p. 129.

Case Law

- "Anvar P.V. v. P.K. Basheer", (2014) 10 SCC 473.
- "Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal", (2020) 7 SCC 1.
- "Tomaso Bruno v. State of U.P.", (2015) 7 SCC 178.
- "Justice K.S. Puttaswamy (Retd.) v. Union of India", (2017) 10 SCC 1.

Statutes and Rules

- Indian Evidence Act, 1872.
- Information Technology Act, 2000.
- Civil Evidence Act, 1995 (UK).
- Federal Rules of Evidence, United States.
- Evidence Act (Singapore), Act 97 of 1893 (as amended in 2012).
- Regulation (EU) No. 910/2014 on electronic identification and trust services (eIDAS Regulation).
- Digital Personal Data Protection Act, 2023 (India).

Reports and Guidelines

- National Institute of Standards and Technology (NIST), Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86, 2006.
- National Institute of Standards and Technology (NIST), Guidelines on Mobile Device Forensics, SP 800-101 Rev. 1, 2014.
- ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories.
- UK Judiciary, Practice Direction on Electronic Disclosure, 2014.
- Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.