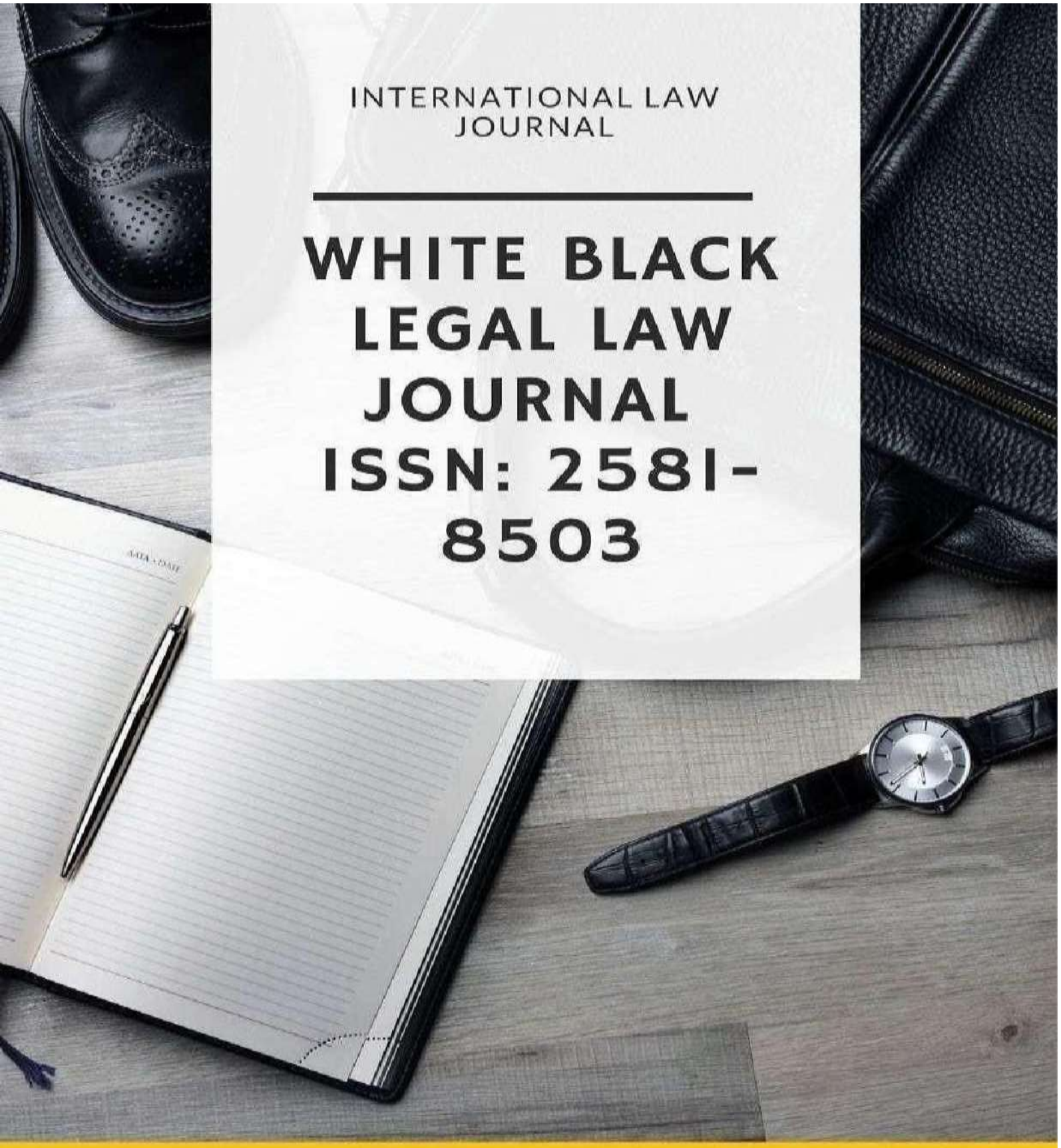

INTERNATIONAL LAW JOURNAL

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 | Aug 2025 ISSN: 2581-8503

AUTHENTICITY AND INTEGRITY OF ELECTRONIC RECORDS: CHALLENGES AND SOLUTIONS IN LEGAL PROCEEDINGS

AUTHORED BY - MANISHA

1. Introduction

The 21st century has witnessed a remarkable shift in the way societies store, access, and exchange information. From handwritten documents and physical records to cloud storage, blockchain databases, and AI-generated content[1], the evolution of information systems has redefined how evidence is created, preserved, and presented in legal proceedings. In this digital paradigm, electronic records have emerged as a central feature of modern litigation, encompassing emails, audio-video files, digital contracts, metadata, mobile phone logs, and even social media posts. This transition, while increasing convenience and efficiency, has also generated new legal and technological challenges, particularly concerning the authenticity and integrity of such records.[2]

Authenticity refers to the assurance that an electronic record is genuine and originates from a reliable and identified source. It involves verifying whether the digital record is exactly what it claims to be and has not been tampered with or forged. On the other hand, integrity deals with whether the record has remained unchanged since its creation or transmission. The challenge in handling electronic evidence arises because digital files can be easily duplicated, altered, or destroyed without leaving visible traces—unlike traditional paper documents. As such, any doubt over the authenticity or integrity of electronic evidence can raise serious concerns about its admissibility and reliability in court.

The legal world, which has long relied on physical forms of evidence governed by well-established rules, has found itself grappling with these novel questions. Courts are now routinely required to assess electronic records presented in civil disputes[3], criminal trials,

[1] Raghavan, Mr Prathap. "Emerging Technologies in Computer Science: AI, IoT, and Blockchain." (2025).
[2] Jindal, Tarun. *Digital and Media Management*. Educohack Press, 2025.
[3] Basu, Subhajit, and Chitra Jha. "Evaluating ICT adoption in the Indian judiciary: challenges, opportunities, and the impact of the e-courts project." *Indian JL & Just.* 15 (2024): 1.

commercial litigations, and constitutional matters. For a judicial system to maintain its credibility and fairness, it must develop rigorous standards to evaluate electronic evidence, particularly to ascertain that it is both genuine and untampered. The emergence of cybercrimes, deepfakes, forged emails, and manipulated surveillance footage further complicates this landscape.

In India, the foundation for recognizing electronic records as admissible evidence was laid down with the enactment of the Information Technology Act, 2000. Sections 3 and 4 of this Act granted legal recognition to electronic signatures and records, respectively. To support this transition in the judicial system, Section 65B of the Indian Evidence Act, 1872, was introduced through an amendment. It specifically laid down the procedure for admitting electronic records, requiring that a certificate accompany any such record to verify its authenticity, mode of production, and source. This certificate plays a crucial role in assuring the court that the evidence is free from tampering and manipulation.

Judicial interpretations of Section 65B have evolved through a series of important rulings. In the landmark case of Anvar *P.V. v. P.K. Basheer (2014)*[4], the Supreme Court clarified that electronic evidence cannot be admitted unless accompanied by the mandatory certificate under Section 65B(4), except where the original device itself is produced in court. This brought much-needed clarity but also gave rise to several procedural hurdles, particularly in cases where the original device was inaccessible or in possession of a third party. This tension between rigid procedural requirements and practical constraints continued until the ruling in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)*[5], where the Court reaffirmed the mandatory nature of the certificate while recognizing the need for flexibility in certain circumstances.

Realizing the need to modernize and simplify evidentiary law in a digital age, the Government of India repealed the colonial Indian Evidence Act and introduced the Bharatiya Sakshya Adhiniyam, 2023 (BSA). This new legislation provides a more comprehensive and updated framework to address the growing relevance of digital evidence. Under the BSA, Section 63 retains the core principles of Section 65B but introduces new concepts such as secure electronic records, presumptions as to digital signatures, and the admissibility of electronic records without production of the original device, provided certain conditions are met. The BSA also

[4] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[5] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

aligns with international practices and seeks to incorporate modern technological developments such as blockchain-based authentication and forensic analysis tools.

Despite these legislative advancements, several practical challenges continue to hinder the reliable use of electronic records in judicial proceedings. The primary challenge lies in ensuring that electronic evidence remains intact throughout its lifecycle—right from creation, storage, transfer[6], to presentation in court. Any gap in the chain of custody or failure to maintain the hash value of the data can cast doubt on its reliability. Moreover, digital records often reside on remote servers or cloud platforms controlled by third-party service providers, which complicates issues of jurisdiction, control, and retrieval.

In addition to integrity concerns, verifying authenticity can be a daunting task, particularly when dealing with anonymous sources, altered metadata, or fabricated content. The rise of AI-generated synthetic media, such as deepfake videos or voice clones, poses a significant threat to the evidentiary process, as traditional forensic tools may not be equipped to detect such manipulation. This calls for not only technical advancement but also legal reform to incorporate specific provisions that address emerging threats in the digital realm.[7]

Globally, legal systems have adopted varying standards to deal with electronic records. The Federal Rules of Evidence (FRE) in the United States, for example, offer a more flexible approach under Rule 901[8], which allows authentication through circumstantial evidence and expert testimony. The eIDAS Regulation in the European Union provides a framework for the use of trusted electronic signatures and digital trust services.[9] Meanwhile, the UNCITRAL Model Law on Electronic Commerce[10] (1996) and Model Law on Electronic Evidence (2019) serve as blueprints for countries seeking to harmonize their national laws with international best practices. These international models stress on technological neutrality, reliability of the method used, and contextual appreciation by courts.

---

[6] Biasiotti, Maria Angela, et al. "Introduction: opportunities and challenges for electronic evidence." *Handling and exchanging electronic evidence across Europe* (2018): 3-12.
[7] Kasper, Agnes, and Eneli Laurits. "Challenges in collecting digital evidence: a legal perspective." *The future of law and eTechnologies*. Cham: Springer International Publishing, 2016. 195-233.
[8] Abraha, Halefom H. "Regulating law enforcement access to electronic evidence across borders: the United States approach." *Information & Communications Technology Law* 29.3 (2020): 324-353.
[9] Hamid, Muhammad Abdullah, Isha Fatima Ifrah Dar, and Nouman Cheema. "Digital Identity and Legal Rights: the EU's eIDAS Regulation as a Model for Global Digital Trust." *Democracy, Rule of Law, and Protection of Human Rights in the European Union* (2023): 88.
[10] Overby, A. Brooke. "Will Cyberlaw be uniform--an introduction to the uncitral model law on electronic commerce." *Tul. J. Int'l & Comp. L.* 7 (1999): 219.

Technological tools such as digital signatures, hash algorithms, timestamping, blockchain ledgers, and cyber forensic software now play a vital role in supporting the authenticity and integrity of electronic evidence. However, their usage requires a certain level of technical literacy among judges, lawyers, and investigating officers. This gap in technical understanding often results in the improper evaluation or outright rejection of electronic records, leading to potential miscarriages of justice. Thus, capacity-building initiatives and judicial training programs are indispensable for equipping stakeholders with the skills needed to handle electronic evidence responsibly and effectively.

In this research paper, a comprehensive examination will be undertaken to explore the legal framework, judicial interpretation, technological standards, and procedural safeguards involved in ensuring the authenticity and integrity of electronic records. The paper will also analyze how the Bharatiya Sakshya Adhiniyam, 2023, addresses these issues and identify gaps that need legislative or institutional attention.[11] Comparative insights from international practices will be drawn to assess the viability of adopting similar standards in India. Finally, the paper will propose a set of policy recommendations and institutional reforms to build a more reliable and robust system for managing electronic evidence in legal proceedings.[12]

By exploring the intersection of law and technology, this study aims to contribute to the growing discourse on digital justice, evidentiary standards, and the evolving responsibilities of courts in the digital age. Upholding the rule of law in an era of bytes and algorithms demands a forward-looking approach that balances the demands of legal formalism with the realities of digital innovation.

2. Challenges in Ensuring Authenticity and Integrity of Electronic Records

Electronic records, unlike traditional paper-based documents, are inherently **fragile, fluid, and vulnerable** to manipulation. Their digital nature, while offering advantages in terms of efficiency, accessibility, and storage, also introduces a host of **legal, procedural, and technological challenges** in maintaining their **authenticity and integrity**. These challenges are critical because electronic records are now widely used in both civil and criminal litigation,

[11] Singh, Vijay Kumar, and Paramjit S. Jaswal. "A Review of Criminal Law Reforms in India: Shaping the Future of Criminal Law in India." (2024).
[12] Bharati, D. R., & Nagarale, D. S. (2024). Digital Forensic Science and Evidentiary Standards in the Bharatiya Sakshya Adhiniyam (BSA) 2023: A Legal Examination of Admissibility.

and their admissibility depends upon proving their genuineness and reliability to the court's satisfaction. The following subsections explore these challenges in depth.

2.1 Vulnerability to Tampering and Alteration

One of the most significant threats to electronic evidence is its **ease of alteration**. Unlike physical documents, which may show visible signs of tampering (erasures, overwriting, torn pages), digital records can be modified without leaving any perceptible trace. A simple metadata change, photo manipulation, or alteration of timestamps can significantly affect the record's evidentiary value. Advanced users can use software tools to edit or fabricate records entirely—this is especially concerning in cases involving financial fraud, cybercrime, or defamation.[13]

This vulnerability raises serious concerns over the **integrity** of digital records—whether they have remained unchanged since creation. The absence of built-in safeguards like digital signatures or cryptographic hash values means that records may not be verifiable. Even emails and WhatsApp messages, often relied on in courts,[14] can be spoofed or altered before being submitted as evidence. Without a robust method of verifying that the data presented is complete and unchanged, courts face difficulties in relying on such records.

2.2 Lack of Metadata Verification and Chain of Custody

Metadata—which includes information such as the date of creation, modification history, file size, location, and creator—plays a crucial role in verifying the authenticity and context of an electronic record.[15] However, courts and even investigating officers often neglect or overlook this aspect, treating only the visible content as evidence. This leads to a scenario where critical circumstantial details, which could confirm or deny a document's credibility, are excluded from judicial scrutiny.

Moreover, the **chain of custody**—the record of who handled the electronic record, when, and how—is crucial in maintaining the integrity of evidence throughout its lifecycle.[16] Any gap or

[13] Suryal, Akarshan. "RETRACTED: Leveraging metadata in social media forensic investigations: Unravelling digital clues-A survey study." (2024): 301798.
[14] Varma, Swrang. "Legality of Serving Summons/Notice through Unconventional Modes of Transmission through Electronic Means." *NUALS LJ* 13 (2019): 88.
[15] Miller, Steven Jack. *Metadata for digital collections*. American Library Association, 2022.
[16] Premanand Narasimhan, Dr N. "Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics." (2024).

break in this chain may give rise to the possibility of tampering. For instance, if a digital video was downloaded by one officer, emailed to another, transferred to a USB drive, and then presented in court, each step must be documented and verifiable. Without such documentation, questions about the record's integrity are bound to arise.

2.3 Inaccessibility of Original Devices and Dependency on Secondary Evidence

One major hurdle in authenticating electronic records is the **inaccessibility of the original electronic device** from which the record was generated. This is particularly true in criminal investigations involving surveillance footage, call data records (CDRs), or information stored on servers located in foreign jurisdictions. When the original device is not available for forensic analysis, the court must rely on secondary evidence like printouts or screenshots.

Under India's earlier legal regime (Indian Evidence Act, 1872), the production of such evidence without satisfying Section 65B led to inadmissibility.[17] Though the **Bharatiya Sakshya Adhiniyam, 2023** allows greater flexibility by not mandating the physical production of the device, it still requires a certificate that validates how the record was generated. Procuring this certificate, especially from service providers or third parties, remains a practical challenge, often leading to delays or the exclusion of critical evidence.

2.4 Digital Signatures and the Problem of Forged Identities

Digital signatures were introduced as a solution to authenticity verification. They use cryptographic algorithms to confirm that a document originated from a particular person and has not been altered. However, their use in India remains limited.[18] In many cases, parties submit unsigned or screenshot-based documents without any verifiable signature or digital trace. Courts then rely heavily on oral testimony or circumstantial evidence to assess reliability.

Additionally, **identity theft** and **forged digital credentials** pose a serious challenge. Emails can be sent from look-alike domains, messages can be generated using AI voice models, and login credentials can be misused. Without proper authentication mechanisms like two-factor verification or blockchain-based logging, it is difficult to conclusively link a digital record to its purported originator.

[17] Poola, Smruti. "Analysis Section 65-B of the Indian Evidence Act, 1872 in Light of the V. Rajaram v. State through Inspector of Police Judgement." *Indian JL & Legal Rsch.* 3 (2021): 1.
[18] Boudrez, Filip. "Digital signatures and electronic records." *Archival Science* 7.2 (2007): 179-193.

2.5 Emergence of Deepfakes and Synthetic Evidence

Perhaps the most alarming development in recent years is the rise of **deepfakes** and **synthetic media**, where AI is used to generate hyper-realistic but fake audio, video, or text content.[19] These pose a direct threat to the authenticity of electronic records, especially in criminal trials involving sexual violence, extortion, political manipulation, or reputational harm. Courts may face enormous difficulty in distinguishing between genuine and fabricated content, especially in the absence of advanced forensic tools.

The legal framework in India is currently ill-equipped to handle such threats. There are no explicit provisions under BSA or IT Act, 2000, that deal with synthetic content. This absence creates a gap in addressing challenges that were virtually non-existent a decade ago but are now common in cybercrime investigations.

2.6 Procedural Gaps and Lack of Uniform Judicial Approach

Another challenge is the **inconsistency in judicial approach** regarding the admissibility of electronic evidence. While the Supreme Court has clarified many issues in landmark decisions, lower courts continue to interpret procedural requirements differently.[20] Some courts insist on strict compliance with certification provisions, while others allow exceptions in the interest of justice. This unpredictability creates confusion among litigants and lawyers, leading to unnecessary delays or rejection of vital evidence.

In addition, many trial courts and law enforcement officers lack **technical expertise** in understanding the nature of electronic records. This results in improper collection, storage, or presentation of digital evidence. Courts also lack the infrastructure to view or analyze digital evidence in formats like raw video files, encrypted PDFs, or forensic reports—further undermining the evidentiary value of such materials.

2.7 Cross-Border Data Issues and Jurisdictional Challenges

Finally, a major modern complication in electronic records is their **transnational nature**. Evidence stored on servers in the United States, managed by European companies, accessed in

[19] Ghiurău, David, and Daniela Elena Popescu. "Distinguishing reality from AI: approaches for detecting synthetic content." *Computers* 14.1 (2024): 1.
[20] Chandra, Aparna, William HJ Hubbard, and Sital Kalantry. "The Supreme Court of India: An empirical overview of the institution." (2018).

India, and transmitted across continents poses serious jurisdictional and procedural issues. Obtaining such evidence through Mutual Legal Assistance Treaties (MLATs) or bilateral agreements is time-consuming and may lead to delays in justice delivery.[21]

These cross-border challenges also raise concerns about compliance with **data protection laws**, **privacy rights**, and **international cyber law** obligations. Courts are often caught in a legal grey zone when balancing these competing interests.

3. Legal Standards in India: The Bharatiya Sakshya Adhiniyam, 2023 (BSA) Framework

The **Bharatiya Sakshya Adhiniyam, 2023 (BSA)** represents a landmark shift in the Indian legal regime governing evidentiary processes.[22] By replacing the **Indian Evidence Act of 1872**, the BSA seeks to modernize the judicial approach to evidence in line with contemporary realities of a **digitally-driven society**. Among the most critical innovations under the BSA are its provisions relating to **electronic records**, reflecting growing reliance on digital documentation in both civil and criminal proceedings. This section explores how the BSA addresses challenges of **authenticity**, **integrity**, **admissibility**, and **procedural safeguards** in relation to electronic evidence.

3.1 Recognition of Electronic Records as Primary Evidence

Sections **61** and **63** of the BSA formally recognize electronic records as "documents" eligible for **primary evidentiary status**[23], provided they originate from a secure source or are accompanied by a valid certificate. This foundational change eliminates earlier confusion over whether such records constituted secondary evidence. Courts can now treat electronically stored information, such as emails, digital contracts, or surveillance footage, as **equivalent to traditional paper documents**, enabling a more seamless legal process.

[21] Singh, Nilay Pratap. *Regulating Cross Border Data Flows: An Assessment of India's Data Localisation Framework*. Diss. National Law School of India University, Bangalore, 2021.
[22] Singh, Vratika, et al. "Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023." *Metallurgical and Materials Engineering* 31.3 (2025): 340-345.
[23] Samaddar, Samrat, and Ankita Roy. "Critical Analysis of the Indian Evidence Act in Accordance with Bharatiya Sakshya Adhiniyam." *Issue 4 Int'l JL Mgmt. & Human.* 7 (2024): 152.

3.2 Certificate of Authenticity (Section 63(4))

To maintain evidentiary reliability, **Section 63(4)** mandates a **Certificate of Authenticity** for electronic records not directly produced from their source device. This certificate must specify[24] the technical details of the device, describe the process used for extraction, and identify the person issuing it. Most importantly, it must affirm that the device was in lawful control and functioned properly at the time of extraction. This provision, resembling the earlier **Section 65B** of the Indian Evidence Act, 1872, addresses fears of **digital tampering** and ensures that courts can trust the document's origin and integrity.

3.3 Statutory Presumptions Regarding Electronic Records (Sections 90–93)

A significant innovation of the BSA is the introduction of **statutory presumptions** in favor of certain electronic documents. **Section 90** presumes that electronic agreements affixed with valid **digital signatures** are authentic. **Section 91** allows courts to presume the **integrity of electronic records** generated in a secure digital environment, and **Section 92** allows for the presumption of **accuracy of digital signatures** when verified through a recognized process. These rebuttable presumptions aim to **lighten the evidentiary burden** on parties relying on digital records while preserving the right to challenge them with credible counter-evidence.

3.4 Admissibility Without Original Device (Section 63(6))

One of the more pragmatic developments under the BSA is that the **production of the original device** is no longer mandatory, provided the accompanying certificate under Section 63(4) satisfies authenticity requirements. This addresses issues raised in earlier judicial decisions like *Anvar P.V. v. P.K. Basheer*[25] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[26], which had imposed strict conditions for admissibility. The current law acknowledges **cloud computing**, **remote access**, and **third-party data storage**, thereby removing impractical barriers to the presentation of digital evidence.

3.5 Digital Signatures and Integrity (Section 93)

Section 93 of the BSA provides a clear legal basis for accepting **secure digital signatures** as evidence of both the **authenticity** and **integrity** of electronic records. This aligns with the

[24] Duranti, Luciana. "The reliability and authenticity of electronic records." *Preservation of the integrity of electronic records*. Dordrecht: Springer Netherlands, 2002. 23-30.
[25] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[26] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

technical framework provided under the **Information Technology Act, 2000**[27], particularly provisions relating to secure electronic procedures. The cryptographic validation offered by digital signatures helps confirm the **identity of the sender** and detect any **unauthorized modifications**, giving courts a strong basis for trust.

3.6 Chain of Custody and Forensic Verification

Though not codified explicitly, Indian jurisprudence places increasing weight on maintaining a **chain of custody** in digital evidence cases.[28] Courts now require documentation of every person or system that handled the electronic record, from its collection to its presentation in court. Forensic experts may be called upon to analyze **hash values**, **metadata**, or **access logs** to confirm that no tampering occurred during this timeline. This ensures **traceability and accountability** at each stage.

3.7 Judicial Discretion and Flexibility

The BSA permits greater **judicial discretion** in the evaluation of electronic evidence. If a party cannot produce the original device or obtain a certificate due to legitimate constraints—such as loss of data or foreign data hosting—the court may still admit the record if it deems it **credible and fair**. This ensures that **substantive justice** is not defeated by **procedural rigidity**, echoing the principle that rules of evidence are meant to aid, not obstruct, truth-finding.

3.8 Interplay with IT Act and Data Protection Laws

The BSA must be read in consonance with the **Information Technology Act, 2000**, especially Sections **65A and 85**[29], which deal with the admissibility and evidentiary value of electronic records. Furthermore, the upcoming **Digital Personal Data Protection Act, 2023**, will introduce new obligations for data security, access control, and lawful processing, thereby impacting how electronic records are managed and presented in court. The **combined operation of these laws** ensures a comprehensive framework for legal adjudication involving digital materials.

[27] Penubadi, Harshavardhan Reddy, et al. "Sustainable electronic document security: A comprehensive framework integrating encryption, digital signature and watermarking algorithms." *Heritage and Sustainable Development* 5.2 (2023): 391-404.
[28] Katkuri, Srinivas. "Legal challenges and lacunas in the digital forensics jurisprudence in India."
[29] Ramesh, Ragavi. "Balancing Protection and Access in Digital Locks: Analysing Recent Amendments in Indian Copyright Law." *Nat'l LU Delhi Stud. LJ* 3 (2014): 84.

3.9 Admissibility of Secondary Electronic Evidence

Section 63(3) acknowledges that secondary evidence—such as photocopies, screenshots, or printouts—of electronic records may be admissible[30] if the original device is **inaccessible or unavailable**. This is particularly useful in cloud computing environments or cybercrime cases where direct access is difficult. However, admissibility is contingent on **reliability standards**, which require corroborative materials such as metadata, timestamps, or corroborative testimony.

3.10 Burden of Proof in E-Evidence Cases

While traditional principles under Sections **101–104** of the BSA apply to the **burden of proof**, the nature of digital evidence often shifts this burden depending on who controls the device or system.[31] If a party with exclusive access to a server or laptop fails to produce essential data or explain discrepancies, courts may invoke **Section 114** to draw an **adverse inference**, assuming evidence was withheld or manipulated.

4. International Standards and Best Practices

Internationally, legal systems have adopted diverse but increasingly harmonized approaches to managing electronic evidence, aiming to ensure authenticity, reliability, and procedural fairness in the digital age. In the **United States**, **Rule 901 of the Federal Rules of Evidence** outlines the standard for authentication, allowing electronic records to be deemed admissible when there is sufficient evidence to support their genuineness.[32] Authentication may be established through **metadata, system logs, expert testimony**, or other circumstantial means. This approach emphasizes flexibility, enabling courts to adapt to technological advancements while maintaining evidentiary integrity.

In the **European Union**, the **eIDAS Regulation (Regulation (EU) No. 910/2014)** sets a unified[33] framework for **electronic identification, authentication, and trust services**. It categorizes electronic signatures into standard, advanced, and qualified signatures, with qualified electronic signatures having the same legal standing as handwritten ones. This

[30] Mason, Stephen, and Daniel Seng. *Electronic evidence*. University of London Press, 2017.
[31] Anthal, Danish. "Digital Evidence's Admissibility under the Bharatiya Sakshya Adhiniyam (BSA): A Comparison with the Indian Evidence Act (IEA) 1872." *Available at SSRN 5233584* (2025).
[32] Frieden, Jonathan D., and Leigh M. Murray. "The admissibility of electronic evidence under the federal rules of evidence." *Rich. JL & Tech.* 17 (2010): 1.
[33] Vanella, Alessandro. *Evolution of Digital Identity in Europe: Experimenting with the eIDAS 2.0 Framework and the EU Digital Identity Wallet*. Diss. Politecnico di Torino, 2025.

regulation bolsters the evidentiary value of digital transactions across member states by ensuring **interoperability and security** in cross-border digital interactions.

At a global level, the **UNCITRAL Model Law on Electronic Commerce (1996)** and the **UNCITRAL Model Law on Electronic Evidence (2021)**[34] provide non-binding but influential standards. These model laws encourage recognition of electronic records as equivalent to paper records, provided they are **accessible, intelligible, and reliable**. They also offer guidance on admissibility, burden of proof, and cross-border data authenticity, forming the basis for digital evidence legislation in many countries.

Together, these international frameworks highlight the growing consensus on the **importance of technical safeguards, judicial flexibility, and procedural clarity** in the digital realm. India's Bharatiya Sakshya Adhiniyam, 2023, aligns with many of these standards, particularly in its emphasis on authenticity certificates, digital signatures, and judicial discretion—positioning the Indian legal system within the broader global trend of evidentiary modernization.

5. Technological Challenges

Despite significant legislative and procedural advancements, the use of electronic records in legal proceedings is fraught with complex technological challenges that threaten their authenticity, reliability, and admissibility.[35] As digital data becomes central to dispute resolution and prosecution, understanding these vulnerabilities is critical for legal practitioners, judicial officers, and policymakers.

Tampering and Fabrication remain primary concerns. With the proliferation of advanced editing tools and forensic software, digital files—whether PDFs, images, emails, or video recordings—can be modified with minimal traceability. Unless electronic records are secured using cryptographic hash functions, tampering may go undetected. Hashing algorithms, which generate unique digital fingerprints for data, can detect even minor alterations. However, unless such hashes are generated and recorded at the time of original storage, they offer limited

[34] Castellani, Luca G. "UNCITRAL texts on electronic commerce." *The Elgar Companion to UNCITRAL*. Edward Elgar Publishing, 2023. 512-524.
[35] ABUSOMWAN, JACOB OSARIEMEN. "CHALLENGES AND PROSPECTS TO THE ADMISSIBILITY OF ELECTRONICALLY GENERATED EVIDENCE." *African Journal of Law, Ethics and Education (ISSN: 2756-6870)* 4.1 (2024).

retrospective utility. Audit trails and version histories maintained by secure digital platforms can help, but not all systems implement these features robustly.

Metadata Manipulation presents another major issue. Metadata, which includes information such as timestamps, location data, and author identity, plays a crucial role in establishing the chain of custody and contextual reliability of electronic evidence.[36] Yet, tools like EXIF editors and metadata scrubbers allow individuals to alter this data easily. Courts and forensic analysts must therefore rely on deep-system forensic techniques and corroborative records to validate claims based on metadata—techniques that may not be accessible in routine legal practice.

Cloud Storage and Jurisdictional Complexities exacerbate evidentiary challenges. As electronic records are increasingly stored on cloud servers distributed across multiple countries, issues arise concerning data sovereignty, access rights, and the legal authority required to compel production. Delays in obtaining mutual legal assistance treaties (MLATs) or fulfilling foreign jurisdiction requirements can undermine the timeliness and admissibility of evidence. Furthermore, establishing a verifiable chain of custody becomes increasingly difficult when data is transferred between third-party service providers across borders.[37]

Deepfakes and AI-Generated Content present perhaps the most formidable emerging threat. Deepfake technologies can fabricate audio, video, and image content[38] with startling realism, making it difficult for courts to distinguish genuine content from manipulated or entirely synthetic media. These developments challenge traditional notions of perception-based evidence and require courts to rely on advanced **digital forensics**, such as noise analysis, biometric verification, or deep learning-based detection algorithms, to assess authenticity.

In sum, the increasing sophistication of technology not only enhances the utility of electronic records but also necessitates **continuous innovation in evidentiary safeguards**, **legal reforms**, and **cross-disciplinary training** to uphold the integrity of digital justice systems.

[36] Suryal, Akarshan. "RETRACTED: Leveraging metadata in social media forensic investigations: Unravelling digital clues-A survey study." (2024): 301798.
[37] Sharma, Shambhavi. "Issues with enforcing Mutual Legal Assistance Treaties (MLATs): Access to cross-border data in criminal investigation." *Available at SSRN 3815270* (2020).
[38] Carpenter, Perry. *FAIK: A Practical Guide to Living in a World of Deepfakes, Disinformation, and AI-Generated Deceptions*. John Wiley & Sons, 2024.

6. Technological Challenges to Authenticity and Integrity of Electronic Records

The authenticity and integrity of electronic records, while crucial in modern judicial proceedings, are increasingly threatened by evolving technological vulnerabilities. As the reliance on digital evidence grows, so do the risks associated with manipulation, misrepresentation, and jurisdictional complexity. This section highlights the key technological challenges undermining the reliability of electronic records in courts.

6.1 Tampering and Fabrication

Digital records are inherently susceptible to tampering. Sophisticated software tools enable alteration of documents, emails, images, and videos without leaving overt signs.[39] Unless cryptographic safeguards like **hash values** are used at the time of creation and storage, such tampering may go undetected. Even minor edits to a file can change its content without altering its appearance. Courts increasingly demand forensic validation using **hash comparisons**, but in the absence of original hash values, proving tampering becomes challenging.

6.2 Metadata Manipulation

Metadata—often referred to as data about data—is essential for establishing the origin, authorship, date, and time of an electronic record. However, free and accessible software allows even laypersons to alter metadata, raising serious concerns about evidentiary reliability. For example, changing the "created" or "last modified" date of a document can mislead investigations or dispute timelines. To counter this, forensic experts may rely on system logs or embedded file attributes, but such analysis is expensive, time-consuming, and not foolproof.

6.3 Cloud Storage and Jurisdictional Complications

Most modern data is stored on cloud servers, often located in foreign jurisdictions. This raises two interrelated problems: access and control. Legal authorities may face delays in obtaining access through **Mutual Legal Assistance Treaties (MLATs)**, and cloud providers may resist sharing data citing data protection laws.[40] This hampers the establishment of a clear **chain of custody** and weakens the evidentiary strength of such data in court proceedings.

[39] Nagra, Jasvir, and Christian Collberg. *Surreptitious software: obfuscation, watermarking, and tamperproofing for software protection*. Pearson Education, 2009.
[40] Sharma, Shambhavi. "Issues with enforcing Mutual Legal Assistance Treaties (MLATs): Access to cross-border data in criminal investigation." *Available at SSRN 3815270* (2020).

6.4 Deepfakes and AI-Generated Content

The emergence of **deepfakes** and **AI-generated media** poses a novel threat to digital authenticity. These technologies can fabricate realistic audio and video clips that mimic real individuals with high accuracy, potentially being misused for character assassination[41], blackmail, or presenting false evidence. Traditional visual verification becomes ineffective, requiring the deployment of **AI detection tools**, forensic watermarking, and pattern recognition technologies to assess the truthfulness of such evidence.

In conclusion, the technological threats to electronic evidence call for an integrated response comprising **judicial training**, **technical safeguards**, **forensic capabilities**, and **strong legislative backing** to ensure that courts continue to function as arenas of truth in an increasingly digital world.

7. Proposed Reforms and Policy Recommendations

As electronic records become central to legal proceedings, India's evidentiary framework must evolve to address emerging technological and procedural challenges. To strengthen the authenticity and integrity of such records, a multi-pronged reform strategy is needed, integrating legal, institutional, and technological interventions. The following policy recommendations are crucial for creating a robust and trustworthy ecosystem for electronic evidence.

1. **Uniform Guidelines for Certification**
   A standardised format and content for authenticity certificates under Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023, should be developed and enforced. Courts across jurisdictions often encounter inconsistent and inadequate certificates, which complicates the admissibility of electronic records. A uniform template with mandatory details—such as device specifications, software used, and digital hash—would enhance reliability, reduce judicial discretion, and promote consistency in evidentiary practice.
2. **Judicial and Prosecutorial Training Modules**
   Regular, compulsory training programs for judges, prosecutors, and investigators in the domains of cyber law, digital forensics, blockchain-based records, and AI-generated content are essential. Without adequate technical literacy, legal professionals may

[41] Gruber, Andreas, and J. D. Robin Pierce. "Transatlantic challenges in access to electronic evidence: Conflicting obligations under the Stored Communications Act and the General Data Protection Regulation." (2019).

struggle to properly assess or challenge electronic evidence. The National Judicial Academy and state judicial academies must integrate specialised modules in collaboration with forensic and IT experts.

3. **Legislative Amendments for Emerging Technologies**

   The legal recognition of AI-generated evidence, data from Internet of Things (IoT) devices, and blockchain-based records is currently ambiguous. Legislative updates must explicitly include these newer categories of electronic evidence under the BSA and IT Act. Clear guidelines should define their admissibility, reliability parameters, and the mode of certification or authentication.

4. **Public-Private Collaboration**

   There is a pressing need for synergy between the legal community and technology stakeholders. Collaborative efforts can help create secure platforms for collection, preservation, and transmission of digital evidence. Industry players can offer insights into encryption standards, digital forensics, and secure logging, which can inform policy and judicial practice.

5. **Creation of Government-Accredited E-Evidence Labs**

   India should establish dedicated digital evidence laboratories modeled on the lines of the National Forensic Science Laboratory (NFSL), but with exclusive focus on electronic records. These labs should ensure robust chain-of-custody protocols, metadata verification, and advanced forensic analysis using AI tools. Such institutions can support law enforcement agencies and courts with credible technical validation of digital evidence.

   Together, these reforms will fortify the legal architecture around electronic records, ensuring that both procedural safeguards and technological realities are meaningfully addressed.

8. Conclusion

The growing reliance on electronic records in judicial proceedings signifies a paradigm shift in evidence law. While statutory frameworks like the Bharatiya Sakshya Adhiniyam, 2023, and the Information Technology Act, 2000, lay down essential principles, rapid technological evolution continues to expose gaps in legislative clarity, procedural adaptability, and forensic infrastructure.

Electronic evidence, unlike traditional forms, is inherently volatile and susceptible to manipulation. Ensuring its authenticity and integrity thus requires a holistic approach that spans secure storage practices, reliable certification, forensic verification, and procedural safeguards. Courts must strike a careful balance—avoiding over-reliance on rigid technical formalities that could exclude valid evidence, while also ensuring that manipulative or fabricated data does not corrupt the justice process.

The integration of judicial training, legislative foresight, technical collaboration, and infrastructural development can collectively address these challenges. As deepfakes, IoT data, and AI-driven content become more common, legal systems must be agile and prepared.

In conclusion, the path forward lies in fostering a resilient digital evidentiary ecosystem—one where law, technology, and institutional capacity converge to uphold justice in the digital age. Only through such synergy can the courts remain trusted arbiters in an era where truth itself can be digitally reconstructed or disguised.

References

Journals / Articles

1. Abraha, Halefom H. "Regulating law enforcement access to electronic evidence across borders: the United States approach." Information & Communications Technology Law 29.3 (2020): 324-353.
2. ABUSOMWAN, JACOB OSARIEMEN. "CHALLENGES AND PROSPECTS TO THE ADMISSIBILITY OF ELECTRONICALLY GENERATED EVIDENCE." African Journal of Law, Ethics and Education 4.1 (2024).
3. Anthal, Danish. "Digital Evidence's Admissibility under the Bharatiya Sakshya Adhiniyam (BSA): A Comparison with the Indian Evidence Act (IEA) 1872." Available at SSRN 5233584 (2025).
4. Basu, Subhajit, and Chitra Jha. "Evaluating ICT adoption in the Indian judiciary: challenges, opportunities, and the impact of the e-courts project." Indian JL & Just. 15 (2024): 1.
5. Bharati, D. R., & Nagarale, D. S. "Digital Forensic Science and Evidentiary Standards in the Bharatiya Sakshya Adhiniyam (BSA) 2023: A Legal Examination of Admissibility." (2024).

6. Biasiotti, Maria Angela, et al. "Introduction: opportunities and challenges for electronic evidence." Handling and exchanging electronic evidence across Europe (2018): 3-12.
7. Boudrez, Filip. "Digital signatures and electronic records." Archival Science 7.2 (2007): 179-193.
8. Chandra, Aparna, William HJ Hubbard, and Sital Kalantry. "The Supreme Court of India: An empirical overview of the institution." (2018).
9. Duranti, Luciana. "The reliability and authenticity of electronic records." Preservation of the integrity of electronic records. Dordrecht: Springer Netherlands, 2002. 23-30.
10. Frieden, Jonathan D., and Leigh M. Murray. "The admissibility of electronic evidence under the federal rules of evidence." Rich. JL & Tech. 17 (2010): 1.
11. Ghiurău, David, and Daniela Elena Popescu. "Distinguishing reality from AI: approaches for detecting synthetic content." Computers 14.1 (2024): 1.
12. Gruber, Andreas, and J. D. Robin Pierce. "Transatlantic challenges in access to electronic evidence: Conflicting obligations under the Stored Communications Act and the General Data Protection Regulation." (2019).
13. Hamid, Muhammad Abdullah, Isha Fatima Ifrah Dar, and Nouman Cheema. "Digital Identity and Legal Rights: the EU's eIDAS Regulation as a Model for Global Digital Trust." Democracy, Rule of Law, and Protection of Human Rights in the European Union (2023): 88.
14. Kasper, Agnes, and Eneli Laurits. "Challenges in collecting digital evidence: a legal perspective." The future of law and eTechnologies. Cham: Springer International Publishing, 2016. 195-233.
15. Katkuri, Srinivas. "Legal challenges and lacunas in the digital forensics jurisprudence in India."
16. Overby, A. Brooke. "Will Cyberlaw be uniform--an introduction to the UNCITRAL model law on electronic commerce." Tul. J. Int'l & Comp. L. 7 (1999): 219.
17. Penubadi, Harshavardhan Reddy, et al. "Sustainable electronic document security: A comprehensive framework integrating encryption, digital signature and watermarking algorithms." Heritage and Sustainable Development 5.2 (2023): 391-404.
18. Poola, Smruti. "Analysis Section 65-B of the Indian Evidence Act, 1872 in Light of the V. Rajaram v. State through Inspector of Police Judgement." Indian JL & Legal Rsch. 3 (2021): 1.
19. Premanand Narasimhan, Dr N. "Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics." (2024).

20. Raghavan, Mr Prathap. "Emerging Technologies in Computer Science: AI, IoT, and Blockchain." (2025).
21. Ramesh, Ragavi. "Balancing Protection and Access in Digital Locks: Analysing Recent Amendments in Indian Copyright Law." Nat'l LU Delhi Stud. LJ 3 (2014): 84.
22. Samaddar, Samrat, and Ankita Roy. "Critical Analysis of the Indian Evidence Act in Accordance with Bharatiya Sakshya Adhiniyam." Issue 4 Int'l JL Mgmt. & Human. 7 (2024): 152.
23. Sharma, Shambhavi. "Issues with enforcing Mutual Legal Assistance Treaties (MLATs): Access to cross-border data in criminal investigation." Available at SSRN 3815270 (2020).
24. Singh, Vijay Kumar, and Paramjit S. Jaswal. "A Review of Criminal Law Reforms in India: Shaping the Future of Criminal Law in India." (2024).
25. Singh, Vratika, et al. "Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023." Metallurgical and Materials Engineering 31.3 (2025): 340-345.
26. Suryal, Akarshan. "RETRACTED: Leveraging metadata in social media forensic investigations: Unravelling digital clues-A survey study." (2024): 301798.
27. Varma, Swrang. "Legality of Serving Summons/Notice through Unconventional Modes of Transmission through Electronic Means." NUALS LJ 13 (2019): 88.

Books / Dissertations

1. Carpenter, Perry. FAIK: A Practical Guide to Living in a World of Deepfakes, Disinformation, and AI-Generated Deceptions. John Wiley & Sons, 2024.
2. Jindal, Tarun. Digital and Media Management. Educohack Press, 2025.
3. Mason, Stephen, and Daniel Seng. Electronic evidence. University of London Press, 2017.
4. Miller, Steven Jack. Metadata for digital collections. American Library Association, 2022.
5. Nagra, Jasvir, and Christian Collberg. Surreptitious software: obfuscation, watermarking, and tamperproofing for software protection. Pearson Education, 2009.
6. Singh, Nilay Pratap. Regulating Cross Border Data Flows: An Assessment of India's Data Localisation Framework. Diss. National Law School of India University, Bangalore, 2021.

7. Vanella, Alessandro. Evolution of Digital Identity in Europe: Experimenting with the eIDAS 2.0 Framework and the EU Digital Identity Wallet. Diss. Politecnico di Torino, 2025.

Statutes

1. Bharatiya Nyaya Sanhita, 2023 (BNSS).
2. Bharatiya Sakshya Adhiniyam, 2023 (BSA).
3. Indian Evidence Act, 1872 (as referenced for comparison).

Case Laws

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
3. V. Rajaram v. State through Inspector of Police, (Referenced in Poola Smruti, 2021).