LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 4, Pages:312-327, July 2025

DIGITAL EVIDENCE AND ITS ADMISSIBILITY IN INDIAN COURTS: CHALLENGES AND EVOLVING JURISPRUDENCE

By- Snekha G[1]

ABSTRACT

In this era of digital age, where every click, message, and transaction leave a trace, digital evidence has become a cornerstone of judicial proceedings in India. Whether it's WhatsApp messages, CCTV recordings, blockchain logs, or metadata, courts today are increasingly relying on electronic records to piece together facts, verify timelines, and identify parties involved in both civil and criminal cases. Picture a situation where a cyberstalking victim shares WhatsApp chat screenshots along with location metadata to support their claim of harassment. These digital traces, when properly authenticated, can help establish patterns of abuse, verify proximity, and strengthen the evidentiary value in court. Even when digital evidence looks convincing, courts won't accept it unless it follows proper legal procedures. This includes submitting a certificate under Section 63 of the BSA that verifies how the electronic record was generated and handled. Additionally, BNSS mandates audio-video documentation during electronic seizures to ensure transparency and prevent tampering. Thus this tension between technological clarity and legal compliance forms the important part of problem in admissibility. This paper analyzes the key challenges, the complexity of obtaining authentication certificates, the fragility of digital data, and the lack of forensic infrastructure in lower courts. The Bharatiya Sakshya Adhiniyam (BSA) now explicitly criminalizes acts like digital impersonation and data theft, reflecting a stronger stance against cybercrime. At the same time, the Bharatiya Nagarik Suraksha Sanhita (BNSS) mandates audio-video recording during electronic seizures, adding a layer of transparency and accountability to

[1]**Intern, Lex Lumen Research Journal.**

investigative procedures. Together, these reforms mark a significant shift toward tech-enabled justice and procedural integrity. The role of expert witnesses is emphasized as crucial in translating technical data into legally digestible formats. Ultimately, this study calls for interdisciplinary collaboration and judicial capacity building to ensure that digital evidence is not just admissible—but reliable, ethical, and fair. As India's legal system adapts to the digital frontier, the admissibility of electronic records must evolve to uphold the integrity of justice. This paper examines the shifting contours of India's legal framework by analyzing key statutes such as the Bharatiya Sakshya Adhiniyam (2023), Bharatiya Nyaya Sanhita (2023), Bharatiya Nagarik Suraksha Sanhita (2023), and the Information Technology Act (2000). Together, these laws reflect India's transition toward a more technology-driven and citizen-centric justice system.

KEYWORDS: WhatsApp chats, electronic records, Bharatiya Sakshya Adhiniyam, Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, Information Technology Act.

INTRODUCTION:

In today's legal environment, the growing integration of digital technologies has reshaped how evidence is collected, presented, and evaluated in courtrooms, marking a significant shift from traditional practices to more data-driven and tech-enabled judicial processes. The increasing reliance on electronic communication, surveillance systems, and data storage platforms has led to a surge in digital records being submitted as evidence in both civil and criminal trials. These records encompass a wide array of formats, including emails, instant messages, CCTV footage, call logs, metadata, and documents stored on cloud servers. Digital evidence has become a foundational element in modern litigation, thanks to its ability to clarify facts, establish timelines, and identify the individuals involved in a case. Its precision and traceability make it an indispensable tool for both civil and criminal proceedings.

Even though digital evidence is becoming increasingly central to legal proceedings, its admissibility in Indian courts remains a nuanced and evolving challenge. Courts must navigate

complex issues of authenticity, certification, and procedural compliance especially under the updated framework of the Bharatiya Sakshya Adhiniyam, which replaces the older Evidence Act and introduces stricter standards for electronic records. The legal system, originally designed to accommodate physical and documentary evidence, has had to adapt to the unique characteristics of electronic records. The Indian Evidence Act, 1872 later amended by the Information Technology Act, 2000 laid the foundational framework for recognizing electronic records within legal proceedings. Sections 65A and 65B were introduced to specifically govern the admissibility of electronic records, with Section 65B requiring a formal certificate that confirms how the digital evidence was produced and by whom. This certification acts as a procedural safeguard to ensure the reliability and integrity of electronic evidence presented in court. However, in practice, these procedural requirements have often led to confusion and inconsistency, making certification under Section 65B a persistent challenge in Indian courts. The recent enactment of the Bharatiya Sakshya Adhiniyam, 2023, attempts to modernize these provisions, yet ambiguities persist.

Judicial interpretation has played a pivotal role in shaping the admissibility standards for digital evidence. Landmark decisions such as *Anvar P.V. v. P.K. Basheer*[2] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[3] have clarified procedural mandates, while also exposing gaps in technical understanding and infrastructural readiness. Moreover, the admissibility process is often hindered by concerns over data authenticity, tampering risks, and the protection of individual privacy under Article 21 of the Constitution.

This paper seeks to critically examine the statutory framework, judicial trends, and practical challenges surrounding digital evidence in India. It also explores the need for systemic reforms, technological innovation, and ethical safeguards to ensure that digital evidence contributes meaningfully to the pursuit of justice in an increasingly digitized society.

[2] Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473
[3] AIR 2020 SUPREME COURT 4908, AIRONLINE 2020 SC 641

TYPES OF DIGITAL EVIDENCE:

REPLICANT DATA: Replicant data refers to duplicate or backup versions of original files, often stored on cloud platforms, external drives, or synced devices. It serves as a fallback when primary data is deleted, corrupted, or inaccessible. Examples of digital evidence include documents that are automatically saved by software, cached versions of websites stored by browsers, and folders that are continuously updated through cloud synchronization services. Replicated data acts like a digital safety net, helping ensure that important information stays intact and accessible even if the original files are lost, damaged, or go missing. By keeping synchronized copies across systems, it supports the smooth flow of data and strengthens the reliability of digital evidence. By maintaining synchronized copies across platforms, it ensures that critical evidence remains available when needed most. It becomes especially valuable when original records are lost, deleted, or corrupted, allowing investigators to recover critical evidence from backup copies and maintain the integrity of the forensic trail. By maintaining backup copies across systems, it ensures that critical records remain accessible even in the face of technical failures or data corruption. Its admissibility depends on demonstrating that the replication process preserved the original content without alteration.

VIDEO FOOTAGE AND IMAGES: Visual evidence such as CCTV recordings, mobile videos, and photographs plays a crucial role in identifying individuals, confirming events, and supporting witness testimony. Digital files often contain embedded metadata such as timestamps, geolocation coordinates, and device identifiers that serve as crucial indicators for verifying authenticity and tracing the origin of electronic evidence. However, for such footage to be admissible in court, it is essential to maintain a well-documented chain of custody and demonstrate that the recording has remained to be accepted in court, the footage must remain untouched from the moment it was recorded until it is presented during trial, with a clear and documented trail showing how it was handled throughout. Courts increasingly rely on such evidence in criminal cases, especially when supported by forensic analysis and expert testimony.

ARCHIVES: Archives are compressed or bundled data sets that preserve historical records. These include ZIP files, email archives, and database backups. They often contain deleted or older versions of documents, making them valuable in uncovering hidden or tampered information. In legal contexts, archives can reveal long-term patterns of communication, financial transactions, or digital behavior. The admissibility of archived digital evidence depends on proving that it was acquired and preserved using forensically sound methods, ensuring its integrity and reliability throughout the investigative process.

ACTIVE DATA: Active data refers to files and information currently accessible on a device, such as documents, spreadsheets, media files, and application data. This category of digital evidence is generally the easiest to locate and examine, making it especially useful during the initial stages of forensic analysis. It reflects the user's ongoing activities and is often used in civil litigation, fraud investigations, and intellectual property disputes. Since active data is not deleted or hidden, it is considered reliable, provided its origin and integrity are verified.

METADATA: Metadata refers to the embedded information within digital files that captures essential details such as creation and modification dates, file size, author identity, and geolocation. Metadata serves as a vital component in digital forensic investigations, offering embedded details such as timestamps, access logs, and modification history that help validate the authenticity of electronic records. This hidden layer of information enables investigators and courts to reconstruct timelines and determine whether a file has been altered or tampered with. By revealing how digital content was created, accessed, and handled, metadata transforms ordinary files into reliable forensic artifacts. Its evidentiary value lies in its ability to support the integrity and admissibility of electronic records, making it indispensable in legal proceedings involving digital evidence. For instance, a document's metadata can reveal whether it was edited after submission or created by someone other than the claimed author. In Indian courts, metadata is increasingly scrutinized alongside Section 65B certification to ensure evidentiary reliability.

RESIDUAL DATA: Residual data, also known as data remnants, consists of fragments left behind after deletion or overwriting. This encompasses elements such as unallocated disk space, file slack, and registry artifacts, which often contain residual data that can be critical in forensic

investigations. Forensic tools are capable of retrieving residual data from sources like unallocated disk space, file slack, and registry artifacts, which can be instrumental in identifying efforts to conceal, alter, or destroy digital evidence. Residual data is particularly useful in cybercrime investigations, where perpetrators may try to erase incriminating evidence. Its admissibility depends on demonstrating that recovery methods did not alter the original content and that the data is relevant to the case.

VOLATILE DATA: Volatile data resides in temporary memory (RAM) and is lost when a device is powered off. It includes running processes, clipboard contents, session cookies, and network connections. Capturing volatile data requires live acquisition techniques and must be done promptly to preserve its integrity. This type of evidence is critical in malware investigations, real-time breach analysis, and insider threat detection. Courts may admit volatile data if its collection is documented and supported by expert testimony.

LOGS: Logs are foundational to digital investigations, offering a chronological trail of system and user activities. These include operating system logs, network traffic records, email headers, and application usage histories. Logs can reveal login attempts, file access, system errors, and communication patterns. Their evidentiary value lies in their ability to reconstruct timelines, verify user actions, and detect anomalies. In court, logs are often used to establish intent, corroborate alibis, or challenge claims of innocence, provided their integrity is maintained through proper forensic handling.

LEGAL FRAMEWORK GOVERNING DIGITAL EVIDENCE IN INDIA

The admissibility of digital evidence in Indian courts is shaped by three key statutes:

the now-repealed Indian Evidence Act of 1872, to the Information Technology Act of 2000, and most recently, the Bharatiya Sakshya Adhiniyam, 2023 each reflecting a step toward modernizing evidentiary standards in the digital age. These laws collectively define how electronic records are recognized, presented, and admitted in judicial proceedings.

1. Indian Evidence Act, 1872 (as amended):

Although originally designed for a pre-digital era, the Indian Evidence Act was later amended through the Information Technology Act, 2000 to incorporate provisions for recognizing and admitting electronic records in legal proceedings.

The scope of 'evidence' under Section 3[4] of the Indian Evidence Act was broadened through amendments to include electronic records, thereby recognizing digital formats as valid documentary evidence in legal proceedings. [5]

To regulate the admissibility of electronic records, two key provisions Sections 65A [4]and 65B[6] were introduced into the Indian Evidence Act through the Information Technology Act, 2000.

Thereby Section 65A served as a general reference to special rules for electronic evidence, while Section 65B laid down specific conditions, including the requirement of a certificate under subsection (4)[7]to validate the record's authenticity.

---

[4] **Interpretation-clause:- Evidence.** -- "Evidence" means and includes—

all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;

[5] **A. Special provisions as to evidence relating to electronic record:**
The contents of electronic records may be proved in accordance with the provisions of section 65B.

[6] **Admissibility of electronic records.** Electronic records stored or printed via computer are admissible as documents if certified under specified conditions, ensuring authenticity, lawful control, proper operation, and accurate reproduction.

[7] In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-(a)identifying the electronic record containing the statement and describing the manner in which it was produced;(b)giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;(c)dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

Further amendments included Section 22A, which limited the admissibility of oral admissions concerning electronic records, and Section 45A, which allowed expert opinion to explain or verify digital evidence. Despite legislative improvements, the system has often been criticized for its rigid procedures and the lack of uniformity in how courts interpret and apply digital evidence standards.

2. Information Technology Act, 2000

The Information Technology Act, 2000 establishes the legal foundation for recognizing electronic records and digital signatures, granting them the same validity as traditional paper-based documents in electronic transactions and legal proceedings.

All documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence.

Section 4[8] equates electronic records with physical documents, ER are legally recognized when information required to be in writing is instead provided in electronic form, as long as it is accessible and usable for future reference.

Section 5[9] of the Information Technology Act, 2000 grants electronic signatures the same legal recognition as handwritten ones, provided they meet the prescribed standards set by the government. These provisions are essential for recognizing digital contracts, communications, and transactions.

[8] **Legal recognition of electronic records.-** Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-(a)rendered or made available in an electronic form; and(b)accessible so as to be usable for a subsequent reference.

[9] Legal recognition of 1 [electronic signatures].—Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of 1 [electronic signature] affixed in such manner as may be prescribed by the Central Government. Explanation.–For the purposes of this section,
―signed, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression ―signature‖ shall be construed accordingly.

While the Information Technology Act, 2000 does not directly govern the admissibility of digital evidence in judicial proceedings, it plays a complementary role by defining and validating electronic records and digital signatures. This statutory recognition ensures that digital content is treated as legally valid, forming the basis for its use in courts. However, the actual rules for admitting such evidence are laid out in evidentiary statutes previously the Indian Evidence Act, 1872, and now the Bharatiya Sakshya Adhiniyam, 2023. Together, these laws create an interdependent framework where the IT Act establishes legitimacy, and the evidentiary statutes determine procedural admissibility.

3. Bharatiya Sakshya Adhiniyam, 2023:

The Bharatiya Sakshya Adhiniyam, 2023 replaces the colonial-era Indian Evidence Act and introduces a modernized framework tailored to the demands of digital communication, electronic records, and contemporary legal challenges. Chapter IV[10] is dedicated to electronic records, and

Section 2(1)(d)[11] the document includes digital records within the definition of evidence. Section 61[12], which corresponds to the repealed Section 65B of Indian Evidence Act, retains the certificate requirement for admissibility but introduces flexibility. Courts may waive the certificate if the record is undisputed and can be authenticated by other means.

The BSA also addresses emerging technologies such as blockchain, digital signatures, and AI generated content, reflecting a shift toward a more adaptive legal system. This evolution marks a significant step toward aligning India's evidentiary standards with the realities of digital litigation.

[10] Of Documentary Evidence

[11] 2(1)(d) "document" means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records.

[12] Electronic or digital record: Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity and enforceability as other document.

CHALLENGES IN ADMITTING DIGITAL EVIDENCE

Despite notable reforms in India's legal framework to accommodate digital evidence, its practical application continues to face serious challenges. These issues arise not only from the technical nature of digital data but also from systemic limitations within the justice delivery system. There remains a significant gap between what the law requires and what stakeholders—courts, law enforcement, and litigants can realistically deliver. This disconnect often leads to procedural delays and uncertainty about the admissibility of electronic records. One of the most persistent hurdles is the certification requirement for electronic records. Under Section 61 of the Bharatiya Sakshya Adhiniyam, 2023, any digital document submitted in court must be accompanied by a certificate. This certificate must confirm that the record was produced from a reliable system and explain the conditions under which it was created. However, when the evidence comes from third-party platforms like WhatsApp, Facebook, or cloud services such as Google Drive or AWS, the party presenting the evidence often lacks access to the system itself. As a result, they cannot generate the required certificate. Service providers, on the other hand, may be slow to respond or unwilling to cooperate due to privacy concerns and jurisdictional limitations. Another major issue is the difficulty in accessing and preserving metadata and device-level information. Metadata can reveal critical details such as when and where a file was created or modified, which helps verify its authenticity. But unless this data is collected using proper forensic tools and preserved according to evidentiary standards, it can be easily altered or rendered inadmissible. Even routine actions like opening or copying a file can compromise its integrity, making it unreliable in court.

In many cases, the handling of digital evidence lacks proper documentation and procedural safeguards, leading to frequent breakdowns in the chain of custody. This chain documents how evidence is collected, stored, and presented, ensuring its reliability. In many cases, electronic records are seized without forensic imaging or proper documentation. This makes it difficult to prove that the evidence hasn't been tampered with, giving the defence room to challenge its credibility and weaken its probative value.

Institutional limitations further complicate the situation. Most district courts do not have access to certified digital forensic labs or trained personnel capable of handling electronic records. Law

enforcement agencies, especially in rural areas, often lack standardized procedures and adequate training in digital evidence collection. While central bodies like CERT-In and state-level cybercrime units provide some support, their coverage is uneven and insufficient to meet the growing demand for digital expertise.

Finally, inconsistent judicial interpretation adds another layer of complexity. Some judges admit electronic records based on oral testimony or circumstantial relevance, while others reject them for not meeting technical requirements. This inconsistency undermines legal predictability and places an unfair burden on litigants who may not be familiar with digital procedures.

In conclusion, accepting digital evidence in Indian courts involves far more than simply meeting legal requirements. It demands a well-prepared institutional framework, technical expertise among stakeholders, and consistent judicial interpretation. Without these elements working in harmony, digital records though potentially powerful can become unreliable and vulnerable to exclusion. To truly benefit from digital evidence, India must invest in infrastructure, training, and procedural clarity. Only then can electronic records serve not just as formal compliance tools, but as reliable instruments for delivering justice in a technology-driven legal environment.

COMPARATIVE JURISPRUDENCE ON DIGITAL EVIDENCE: LESSONS FOR INDIAN REFORM

India has made notable strides in updating its legal framework to accommodate digital evidence, especially with the introduction of the Bharatiya Sakshya Adhiniyam, 2023. However, despite these reforms, the system still struggles with procedural rigidity and inconsistent application. In contrast, countries like the United Kingdom and the United States have adopted more flexible, functionality-driven approaches that focus on the reliability of evidence rather than strict procedural compliance.

In the United Kingdom, digital evidence is governed by laws such as the Civil Evidence Act, 1995 and the Criminal Justice Act, 2003. These statutes emphasize the authenticity and reliability of electronic records without mandating rigid certification requirements. Courts in the UK rely on

supporting documentation, expert testimony, and circumstantial evidence to assess digital records. This allows judges greater discretion while still maintaining evidentiary integrity, making the system more adaptable to real-world complexities.

In the United States, the admissibility of digital records is guided by the Federal Rules of Evidence, especially Rules 901 and 902. These provisions emphasize proving that the electronic material is genuine and trustworthy. Instead of relying on rigid formalities, courts assess elements like metadata, forensic evaluations, and the documented handling of the evidence to confirm its authenticity. Rule 902 also allows certain types of digital records to be accepted without additional testimony, provided they come with a certification from a qualified individual. This flexible system helps streamline proceedings while maintaining the reliability of electronic evidence. A key development came with Rule 902(14), introduced in 2017, which allows certain digital records to be self-authenticating if accompanied by a certificate from a qualified person. This approach is more flexible than India's mandatory certification model and reflects a trust-based system that balances forensic rigor with practical efficiency. What truly sets the UK and US apart is not just their legal language but the institutional support behind it. Judges, lawyers, and law enforcement officials in these countries receive regular training in digital forensics. Their courts interpret laws with a focus on the evidentiary value of digital records rather than technical perfection. This ensures that reliable evidence is not excluded due to minor procedural lapses, thereby promoting justice over formality.

India's Bharatiya Sakshya Adhiniyam, 2023 builds upon the foundational structure of the earlier Indian Evidence Act, 1872, while introducing modern updates to reflect contemporary legal and technological realities. While the new law acknowledges the importance of digital records, it still leans heavily on mandatory certification under Section 61. This can be a barrier when dealing with third-party platforms or cloud-based services, where the presenting party may not have access to the system that generated the data. To move forward, India could benefit from adopting global best practices such as allowing flexible authentication methods, investing in forensic infrastructure, and empowering judges with greater discretion. And to conclude, India's journey toward effective digital evidence jurisprudence is ongoing. By learning from the UK and US models, India can shift

from a compliance-heavy framework to one that prioritizes justice, reliability, and accessibility. Such reforms would not only strengthen the credibility of digital evidence but also enhance the overall fairness of the legal process in the digital age.

India's legal treatment of digital evidence has undergone significant transformation, yet it continues to face procedural rigidity and inconsistent implementation. In contrast, common law jurisdictions such as the United Kingdom and the United States offer more flexible and functionality-driven models that prioritize evidentiary reliability over formalistic compliance.

In the United Kingdom, electronic records are admitted in legal proceedings under frameworks such as the Civil Evidence Act of 1995 and the Criminal Justice Act of 2003, which emphasize reliability and authenticity over rigid formalities. These statutes adopt a pragmatic approach, emphasizing the authenticity and reliability of digital records rather than imposing rigid procedural requirements. Courts in the UK do not require a certificate akin to India's Section 65B or Section 61. Instead, authenticity may be established through supporting documentation, expert testimony, or circumstantial evidence. This allows for judicial discretion without compromising evidentiary scrutiny. The United States follows the Federal Rules of Evidence (FRE), particularly Rules 901 and 902, which permit the admission of electronic records if the proponent can demonstrate that the item is what it purports to be. Courts routinely assess metadata, chain of custody, and forensic reports to verify authenticity. Notably, Rule 902(14), introduced in 2017, allows certain digital records to be self-authenticating when accompanied by a certificate from a qualified individual. This mechanism is more flexible than India's mandatory certification model and reflects a trust-based approach to forensic validation.

What sets the UK and US apart is not merely statutory language but the institutional infrastructure supporting digital evidence. Judges, lawyers, and law enforcement personnel receive regular training in digital forensics, and courts adopt a purposive interpretation that values the probative strength of evidence over procedural perfection. This approach helps ensure that valid and trustworthy evidence is not dismissed solely due to minor procedural errors.

India's Bharatiya Sakshya Adhiniyam, 2023 reflects a continuation of the foundational principles laid down in the Indian Evidence Act, 1872, but also presents a timely opportunity for modernization. To make digital evidence more accessible and reliable, India can benefit from adopting global best practices—such as flexible standards for verifying authenticity, stronger forensic infrastructure, and empowering judges with greater discretion. These changes would help shift the current system away from rigid procedural formalities toward a more balanced and justice driven approach. By focusing on practical reliability rather than strict compliance, the legal framework can better accommodate the realities of digital data. Such reforms would not only improve the credibility of electronic records but also make justice more accessible in an increasingly digital society.

RECOMMENDATIONS

Despite recent legislative updates, India's framework for handling digital evidence still faces serious challenges. These issues are not just technical. They stem from procedural rigidity, limited infrastructure, and inconsistent judicial interpretation. To ensure that digital records serve justice rather than hinder it, a more adaptive and robust system is needed.

One of the first areas requiring attention is the certification process under Section 61 of the Bharatiya Sakshya Adhiniyam, 2023. Currently, parties must produce a certificate to validate electronic records, even when the data originates from third-party platforms like WhatsApp, Google Drive, or AWS systems they don't control. This creates a compliance bottleneck. A more practical solution would be to introduce standardized certificate formats and allow courts to waive certification in low-risk cases where authenticity is otherwise evident. Judicial discretion, when exercised with care, can prevent unnecessary exclusion of reliable evidence. Equally important is the need to strengthen India's forensic infrastructure. Most district courts lack access to basic digital forensic tools, and law enforcement agencies often operate without standardized protocols. Establishing district-level forensic labs, deploying mobile forensic units, and equipping courts with hash verification and imaging tools would significantly improve the handling of digital records.

These upgrades must be paired with structured training programs for judges, lawyers, and police personnel focusing on metadata analysis, chain-of-custody procedures, and emerging technologies like blockchain and AI-based verification.

To ensure consistency across jurisdictions, India should adopt uniform guidelines for collecting, preserving, and presenting electronic evidence. Maintaining a documented chain of custody from the point of evidence collection to its presentation in court is crucial to preserving its credibility. Without this, digital records may be challenged for tampering or manipulation, potentially undermining even strong legal cases.

Another critical reform involves improving cooperation with technology platforms. Service providers often delay or deny access to records due to privacy concerns or jurisdictional barriers. A central legal authority perhaps under the Ministry of Home Affairs or CERT-In—could act as a liaison to streamline requests, ensure compliance with cross-border data laws, and reduce procedural delays. Judicial interpretation also needs recalibration. Trial courts often differ in how they apply certification rules for electronic records. As Some accept and reject digital evidence based on compliance and there were inconsistency creates. Clear procedural guidance from higher courts can help standardize practices across jurisdictions. Such clarity would ensure that genuine evidence is not dismissed over minor procedural gaps. Finally, all reforms must respect constitutional safeguards. The process of collecting digital evidence must uphold the constitutional guarantee of privacy under Article 21, ensuring that any intrusion into personal data is lawful, necessary, and subject to judicial oversight. Any intrusion into personal data should be subject to judicial oversight and follow the principles of legality, necessity, and proportionality. Striking the right balance is essential to ensure that technological advancement enhances justice without compromising individual freedoms.

In essence, India must move beyond a rigid, certificate-centric model and embrace a justice-oriented framework one that values transparency, technical competence, and evidentiary fairness.

Only then can digital evidence truly serve its purpose in a modern legal system.

CONCLUSION

Digital evidence now plays a vital role in modern legal proceedings, reflecting how deeply technology has reshaped the way people communicate and interact. India's legal framework progressing from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 demonstrates commendable efforts to recognize and regulate electronic records. Yet, procedural rigidity, infrastructural gaps, and inconsistent judicial interpretation continue to hinder effective implementation. The mandatory certification model, while aimed at ensuring authenticity, often imposes impractical burdens, especially in cases involving third-party platforms or decentralized data. Comparative jurisprudence from countries like the UK and USA shows that flexibility, functional authenticity, and robust institutional support can strengthen evidentiary integrity without undermining justice. For India to fully harness the power of digital evidence, reforms must extend beyond legislation to include technical training, forensic infrastructure, cooperative mechanisms with service providers, and a purposive judicial approach. Bridging the divide between law and technology will be essential in ensuring that digital evidence serves not only as a tool of compliance but as a vehicle for fairness and truth in a digitized legal landscape.

REFERENCES:

1. https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf
2. https://indiankanoon.org/doc/7683886/
3. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
4. https://www.indiacode.nic.in/showdata?actid=AC_CEN_3_20_00034_187201_1523268871700&orderno=3
5. https://www.salvationdata.com/knowledge/8-types-of-digital-evidence/
6. https://indiankanoon.org/doc/172105947/
7. https://indiankanoon.org/doc/487818/