Promoting Judicial Acceptance of Electronic Evidence Through Structured Legal Reform

Navneet Kumar Bharti[1], Dr. Neeru Gupta[2]

[1]Research scholar, [2]Associate Professor (Research Supervisor)
shri Venkateshwara University,Gajraula Amroha (UP)

Abstract:
Modern court processes cannot function without electronic evidence due to the growing dependence on digital technology. But procedural conservatism, judges' lack of technical knowledge, and the lack of consistent standards still make it difficult for Indian courts to accept such evidence, which means important evidence gets ignored and justice isn't served. If we want electronic evidence to be more trustworthy and admissible in court, this paper says we need a legal reform framework that strikes a compromise between formal protections and practical flexibility. Modifications to Section 65B of the Indian Evidence Act, investment in digital evidence examination units and other technological infrastructure, interdisciplinary collaboration among legal, technical, and policy experts, and judicial capacity building through targeted training are the five pillars that make up the proposed model. The goal of this reform paradigm is to make the judicial system more open, accountable, and efficient by fixing underlying problems. In order to guarantee that everyone has equal access to justice in our increasingly digital world, it is crucial to promote the acceptance of electronic evidence by the judiciary. This is not just a technological need, but also a democratic imperative. To strengthen the rule of law and safeguard the rights of victims who depend on electronic data for legal recourse, the report stresses the critical necessity of integrated reforms that provide courts with the knowledge and skills to handle the intricacies of digital evidence.

Keywords: Electronic Evidence, Indian Evidence Act, Judicial Reform, Digital Forensics, Legal Admissibility.

I.INTRODUCTION

Every aspect of contemporary life, including the presentation, shape, and nature of evidence in court processes, has been impacted by the increasing dependence on technology in the digital era. Emails, digital photos, surveillance video, phone records, social media postings, metadata, and other data saved or sent digitally are becoming more common in the legal system. The efficient identification and handling of such evidence is now fundamental for the fair administration of justice due to the increasing number of digital contacts in both civil and criminal proceedings. However, the conceptual, procedural, and technological difficulties offered by electronic evidence are still a problem for India's legal system, even though it has been acknowledged by legislation and has been precedented by courts. Concerns about the validity, dependability, and admissibility of digital evidence, together with the increasing number of cases incorporating it, highlight the critical need for organized legal change to resolve these issues. The Indian Evidence Act of 1872 and its interplay with the Information Technology Act of 2000 formed the primary basis for the present system controlling electronic evidence in India. Electronic records are fundamentally allowed to be presented in court under Section 65B of the Indian Evidence Act. Due to different interpretations and practical problems in getting the necessary certification, the specialized certification procedure as required by this section for digital recordings to be accepted as supplementary evidence sometimes creates a procedural bottleneck. The decision in the seminal case of Anvar P.V. v. P.K. Basheer (2014) upheld the importance of this certificate and dismissed previous interpretations that were more lenient. Despite its good intentions, this strict criterion has unintentionally led to the exclusion of pertinent digital evidence, especially in cases where the party depending on the evidence cannot access the original electronic source or where the custodians refuse to offer the required certification.

Also, the way judges think about electronic evidence has changed over the years. Due to a lack of technical skill, unfamiliarity with digital forensics, or fear of manipulation, some courts have shown reluctance to accept digital evidence, while others have done so with progressive interpretation and reasonable rationale. Uncertainty in the law, delays in procedures and even a miscarriage of justice have resulted from this discrepancy. Thus, the problem is structural and institutional as well as legal, necessitating an all-encompassing strategy that takes into account technology flexibility, judicial competency, and procedural clarity. A number of countries' legal frameworks for dealing with electronic evidence are now more unified and grounded in technology. For example, the Federal Rules of Evidence in the US and the Civil Evidence Act, 1995 in the UK both offer relatively straightforward processes for admitting electronic documents, with an emphasis on the relevance and reliability of the evidence rather than strict procedural mandates. Indian constitutional and procedural authorities may learn a lot from these systems, which strike a good balance between digital documentation's practicality and the necessity for legitimacy. Beyond only streamlining procedures, the use of electronic evidence by the judiciary is critical to maintaining justice's relevance in an ever-evolving society. Digital evidence, for example, may play a crucial role in the criminal justice system in establishing guilt or innocence, tracing illegal actions, or re-creating events.

Digital documentation is crucial for the settlement of civil disputes since more and more contracts, conversations, and transactions are taking place via electronic platforms. Public faith in the legal system is intimately related to the accuracy with which courts can assess this kind of evidence. The three interrelated goals of structured legal reform are as follows:(1) making electronic records more easily admissible by reviewing Section 65B;(2) increasing judges' knowledge and skill in digital evidence and forensic practices through consistent training; and(3) creating consistency across courts by updating bench books and judicial guidelines. In order to build a legal ecosystem that can adapt to new circumstances and face the future head-on, reform efforts should include forensic specialists, technologists, academics, and practitioners. In addition, with the help of standard operating procedures (SOPs), courts may create digital evidence management systems that make it easier to securely handle and evaluate electronic data. Judicial reform and digital justice delivery must coexist in India at this pivotal moment. Along with substantive and procedural improvements that enhance the evidential value of electronic documents, the digitization of court records, virtual hearings, and e-filing should be implemented. Achieving justice system efficiency, openness, and fairness requires more than simply a technical exercise; it requires promoting judicial acceptance of electronic evidence. If this change does not take place, the courts' credibility and the rights of litigants will be undermined as the law becomes obsolete due to technological advancements.

II.CONCEPTUAL FRAMEWORK OF ELECTRONIC EVIDENCE

In judicial proceedings, any data or information that is saved, sent, or processed digitally may be offered and relied upon as electronic evidence. It includes a broad variety of sources, some of which are organized (like databases, log files, and transaction records) and some of which are unstructured (like emails, social media posts, videos, IMs, and papers saved on digital devices). Electronic records have unique qualities that set them apart from more conventional forms of evidence, such as physical papers or witness statements: they are immaterial, easily changed or destroyed, and often found in a scattered or temporary setting. Their unique characteristics add complexity and change to the way they are treated by the law. The four cornerstones of admissible evidence in legal philosophy are dependability, authenticity, materiality, and relevance. Nevertheless, when applied to digital forms, same concepts need a fresh look and a different interpretation. Hash values, metadata, or digital signatures often serve as witnesses in digital cases, although in conventional situations, a witness is still needed to testify to the legitimacy of a document. A technologically informed and procedurally adaptable legal framework is required due to the transient nature of digital records and the need of technology instruments for accessing, verifying, and presenting such material.

Current Legal Framework in India

As digital technology has grown and electronic conversations and records have become more important in both civil and criminal proceedings, India's method for dealing with electronic evidence has evolved significantly. Nevertheless, there are still interpretive and procedural obstacles since the present legal system is based on laws that were developed before the digital age. Due to the ever-changing nature of electronic

data, the current legal system must now find a way to bring conventional evidentiary standards into harmony with them.

The Indian Evidence Act, 1872

The Indian Evidence Act, 1872 is the principal regulation controlling evidence in Indian courts. It was established long before computers and digital communication was commonplace. Sections 65A and 65B, added to the Act in 2000, provide specific guidelines for the admission of electronic documents and make it possible to include them into a case. In specifically, Section 65B lays forth the requirements for the admissibility of electronic documents as supplemental evidence in court. Any such electronic evidence must be accompanied by a certificate under Section 65B(4). The information on this certificate must include:

- The process followed to create the electronic record;
- Specifics of the equipment that was used to create the record;
- Verification that the record was created during routine operations;
- Guarantee that the record is accurate and legitimate.

There is a procedural bottleneck in the digital evidence system since the electronic record is inadmissible if this certificate is not produced, regardless of its relevance or probative value.

The Information Technology Act, 2000

The Information Technology Act, 2000 was created to supplement the Indian Evidence Act and to handle more general issues pertaining to the online environment. The use of digital technology in government, business, and communication is made easier by this act, which gives electronic documents and digital signatures legal standing. Digital authentication via accredited authority is made possible, and a legislative framework is set up to ensure safe electronic transactions. The IT Act strengthens the credibility and admissibility of electronic evidence by defining secure digital signatures and electronic records. The Act also gives the government the authority to establish regulations for digital infrastructure, cybercrimes, and data security.

Section 65B – A Legal Bottleneck

Section 65B of the Indian Evidence Act has been the most disputed and examined by the courts among all of its sections. Electronic evidence admittance has become much more complicated due to the certificate requirement under Section 65B(4). Someone with legitimate authority over the equipment that created the electronic record must issue this certificate. It may be rather difficult, if not impossible, to get the necessary certificate for some types of data, including social media postings, mobile phone recordings, surveillance video, and data obtained from third-party servers (such as Google, Meta, or cellular providers). This leads to the frequent exclusion of crucial evidence based on technicalities, which undermines the pursuit of justice.

Key Judicial Interpretations

In many seminal decisions, India's highest court has upheld the validity of digital evidence, hence reiterating the need of Section 65B's procedural requirements:

- **Anvar P.V. v. P.K. Basheer (2014)**: This historic decision reversed the previous opinion in State v. Navjot Sandhu (2005) and made it very clear that Section 65B is a full code on its own, and that secondary evidence, including oral testimony, cannot be used until the certificate under Section 65B(4) is shown. No matter what happens with the original equipment, the certificate is still necessary for electronic recordings to be admissible, according to the Court.
- **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)**: The Supreme Court reiterated that a Section 65B certificate is strictly required and made it clear that a party has to ask the court to force the person in possession to provide the certificate if it does not have it. There are valid concerns about access to justice since this court upheld the certificate's required character and emphasized the importance of procedural compliance above equitable considerations.

III.CHALLENGES IN JUDICIAL ACCEPTANCE

Despite being a necessary evil in this information age, the Indian court system has hit a number of significant obstacles on the path to incorporating electronic evidence. Not only do legal and procedural inadequacies contribute to these issues, but the judicial process also has constraints in terms of infrastructure, technology,

and interpretation. Some of the main problems that prevent electronic evidence from being accepted by Indian courts without a hitch are as follows:

Procedural Rigidity

Section 65B of the Indian Evidence Act imposes rigid procedural requirements, most notably the necessary certificate under sub-section (4), which poses a significant obstacle. Courts have been forced to dismiss digital evidence only because it lacks this technical certificate, even when its legitimacy and probative value are completely clear. As a result, the law has become too formalized and strict, putting formality ahead of actual justice. In instances when third parties (such telecom providers or social media platforms) have the data, the necessary certification is nearly hard for plaintiffs to provide due to the procedural straitjacket, which has disproportionate implications. This undermines the justice system and gives perpetrators more confidence when they are able to evade prosecution in situations involving cyber bullying, cybercrime, digital banking fraud, and online defamation.

Lack of Judicial Expertise

The judiciary's severely lacking technical knowledge of digital systems, EDSs, and forensic authentication methodologies is another major roadblock. When it comes to determining the trustworthiness and authenticity of electronic documents, many judges and lawyers still don't understand fundamental ideas like digital signatures, metadata analysis, log files, digital hashing, and encryption standards. Because of this disparity in technological understanding, people tend to either blindly follow procedures or accept electronic records without question. Both cases had results that cast doubt on the reliability and equity of the trial. To make matters worse, courts do not have the proper skills to deal with the intricacies of digital evidence because of a lack of formal education in cyber law and digital forensics.

Absence of Uniform Guidelines

One major flaw is that there aren't any national standards for how to properly preserve, present, and handle electronic evidence. From its initial gathering at the site of the crime to its subsequent forensic examination, storage, and presentation in court, digital evidence goes through a lot of stages without a universally accepted framework or standard operating procedure (SOP). As a result, many trial courts, forensic labs, and police agencies have developed their own unique protocols, leading to inconsistencies in the law. This lack of consistency and predictability in the judiciary's rulings begs the question of whether or not the evidence presented is reliable and admissible. The evidential process is still disjointed and vulnerable to procedural gaps since there is no single regulatory mechanism or monitoring authority.

Susceptibility to Manipulation

Data stored in an electronic format is inherently susceptible to manipulation, loss, duplication, and fabrication. Digital records, in contrast to physical ones, may have their contents changed without anyone noticing. There is a significant danger to the trustworthiness of electronic evidence due to its inherent fragility and instability. Digital evidence cannot be shown to be real and uncorrupted due to weak chain-of-custody protocols and inadequate usage of modern forensic validation methods like hash verification, blockchain-based time stamping, and secure server logs. It is common for courts to receive electronically stored documents that have been altered, changed selectively, or obtained from unreliable sources, casting doubt on their admissibility. False or deceptive electronic submissions may undermine public faith in the court process unless forensic infrastructure and strict protections are in place.

IV.STRUCTURED LEGAL REFORM: A THEORETICAL PROPOSITION

India urgently needs a thorough and future-oriented legislative reform plan to address the growing concerns about the credibility and admissibility of electronic evidence. While protecting the integrity of evidence, a theoretically sound reform framework must be pragmatically flexible enough to avoid impeding justice via the strict application of the law. This is why we provide a five-pronged approach that incorporates new laws, enhanced capabilities, improved infrastructure, industry-wide standards, and cross-sector partnerships. In order to better handle the intricacies of digital evidence, each pillar is designed to strengthen the legal ecosystem.

Legislative Reform

- The need to update antiquated legislative laws and incorporate modern legal concepts is central to the change. Here are some suggested changes:

- In situations when getting the required certificate is very difficult, such as when data is stored on servers belonging to third parties, such as foreign platforms or service providers, the Indian Evidence Act should be amended to provide judicial discretion (Section 65B). Justice for everybody and the integrity of evidence would be upheld if this were to happen.
- Electronic documents created and kept in safe digital environments should be presumed to be legitimate, especially if the underlying system is ISO-certified or adheres to internationally accepted cryptography and security standards. As a result, fewer frivolous lawsuits involving questions of authenticity in everyday disputes would arise.
- Pass legislation that defines a "digital chain of custody" and mandates that all entities involved in the processing of evidence must record and verify its transfer; this would guarantee the evidence's integrity and traceability from collection to presentation in court.

Judicial Capacity Building

- The capacity of judges and lawyers to navigate technological changes is contingent upon their familiarity with and skill using digital tools. To strengthen the capacity of the legal system, we should:
- Make it mandatory for judges, prosecutors, and defense attorneys to undergo training in cyber forensics, digital authentication techniques, metadata analysis, hashing protocols, and digital chain-of-custody principles.
- Incorporate modules on digital evidence and cyber law into the curricula of law schools, judicial academies, and bar training programs. This will ensure that technological competence is ingrained in legal education and judicial functioning.

Technological Infrastructure

- The court system needs state-of-the-art technology infrastructure to back up a strong judicial approach to electronic evidence. Important tasks should encompass:
- Data recovery, metadata authentication, and integrity validation tools should be made available to each High Court and significant subordinate court via the establishment of Digital Evidence Examination Units (DEEUs). These units should be manned by qualified digital forensic analysts.
- To ensure that data stays tamper-proof and verifiable throughout its evidential lifespan, it is important to use measures such as secure time stamping, blockchain technology, and hashing algorithms (e.g., SHA-256).

Development of National Standards

- The likelihood of uneven evidence techniques and unpredictable court rulings rises when there is no standardization. Accordingly, national standards is an essential reform component:
- Creating SOPs for the gathering, storage, and presentation of digital evidence, based on world-renowned models used by organizations like INTERPOL, ENISA, and NIST (National Institute of Standards and Technology, USA).
- The establishment of court-supervised digital evidence repositories that can safely store evidence that is sensitive or poses a high risk. Maximum security and transparency should be achieved by these repositories via the use of end-to-end encryption, access logs, and two-factor authentication. Additionally.

Interdisciplinary Collaboration

- A multidisciplinary approach is necessary for successful legal reform due to the growing integration of law and technology. To ensure the legal structure is robust enough for the future, interdisciplinary cooperation is essential:
- The establishment of long-term committees and advisory boards made up of cyber forensic specialists, judges, policy analysts, legal academics, and technologists; their mission: to create context-sensitive legal standards that can adapt to new technology as it develops.
- Encouraging academic research, public-private collaborations, and cross-sectoral interaction to create evidence-based legal frameworks that take into account the ever-changing digital world and proactively address emerging possibilities and dangers.

V.SOCIO-LEGAL IMPLICATIONS

An efficient and adaptable legal framework for electronic evidence is now crucial in a world where digital transactions, virtual communications, and online interactions are becoming the norm. Everything that people do these days leaves a digital trail, whether it's making a purchase, signing a contract, exchanging emails, or

interacting with friends and family. As a result, these traces play a critical role in both civil litigation and criminal prosecution. Therefore, courts should be well-equipped both technically and institutionally to evaluate and accept electronic records in a way that respects the ideals of equity, fairness, and due process.
Significant socio-legal gains may be achieved across several domains by enhancing the court acceptance of electronic evidence:

- **Transparency**: Emails, transaction records, video from security cameras, and data from phone calls all serve as digital records that provide evidence that is objective, time-stamped, and accessible. These data trails may be used as definitive signs of what happened, limiting room for guesswork or personal opinion. The increased openness of public affairs and judicial procedures is a direct result of the increased admissibility of such data.
- **Accountability**: Particularly in areas like corporate regulation, public administration, governance, and law enforcement, the efficient use of electronic evidence increases institutional responsibility. To ensure that people and organizations are held accountable for their activities, digital audits, CCTV video, bodycam recordings, and server logs may be vital in demonstrating accountability.
- **Efficiency**: Records and case files digitized may greatly alleviate administrative responsibilities, logistical limits, and delays in procedures. Particularly in high-volume or time-sensitive cases, courts that enable the smooth integration of electronic evidence into legal procedures enjoy the advantages of simplified processes, quicker decision-making, and enhanced resource management.

The use of electronic evidence is crucial for victims of cyberstalking, cybercrime, financial fraud, cyberimpersonation, online defamation, and abuse that is assisted by technology. There is often a lack of tangible or written proof in these kinds of situations. Unknowingly, these victims are deprived of justice by a legal system that lacks the necessary skills to accept or evaluate digital recordings, or that utilizes procedural formalities to dismiss legitimate evidence. The public's faith in the judicial system is weakened, and access to legal remedies is jeopardized.
Therefore, it is not only a technical exercise to advocate for changes in electronic evidence law, institutions, and technology. It is an essential democratic need for maintaining the availability, equity, and responsiveness of justice in the modern period. As technology and the law evolve in tandem, it is critical that electronic documents be admissible, intact, and evaluated correctly in today's rule of law system.

VI.CONCLUSION

Justice in the digital age cannot be guaranteed without the acceptance and efficient use of electronic evidence. To keep up with the ever-changing demands of digital litigation, India's legal system needs major overhauls, even though it has essential provisions in the Information Technology Act and the Indian Evidence Act. Section 65B, conflicting court interpretations, and technical restrictions all work together to make it harder to trust and admit vital digital data. To get past these obstacles, organized legal reform has to streamline procedures, strengthen investigative and judicial powers, and provide uniform criteria for the assessment of digital documents. Training, infrastructure assistance, and clear legal guidelines are necessary to increase the trust of judges in electronic evidence. Such evidence may be further strengthened by incorporating forensic and technological ideas and learning from the experiences of other jurisdictions. Public faith in the justice system and court efficiency may both be enhanced by enhancing the electronic record system's evidential foundation. To keep Indian courts strong and responsive in this digital age, we need a strategy that is balanced, forward-thinking, and tech-savvy.

REFERENCES:

1. Askarzadeh, G., & Rouhi, A. (2022). Herding behavior in the cryptocurrency market. *Journal of Financial and Behavioral Research in Accounting, 4*(7), 123–135.
2. Babakhani, R. (2012). A study on the evidentiary value of electronic documents in Iranian law. *Islamic Law Research Journal, 1*(35), 157–188.
3. Baghani, E. (2020). Examining the oversight mechanisms for new financial technologies: FinTech and cryptocurrency. *Investment Knowledge Journal, 9*(35), 153–168.
4. Ghajar, S. (2002). Introduction to public key infrastructure. *Informatics Newsletter, 85*, 57–89.

5. Ghorbani, F., & Mousavi, Z. S. (2021). The impact of cryptocurrency, Bitcoin, and digital currency on financial interactions in modern businesses. *International Conference on Management and Humanities Research in Iran, 2*(9), 210–223.
6. Khordmand, M. (2019). A jurisprudential study of cryptocurrency mining and exchange with a focus on the 'Bitcoin' network. *Islamic Economics Knowledge Journal, 2*(20), 109–124.
7. Matsura, J. H. (2018). Overview of cryptocurrency regulations and their legal implications. *Civilization Law Journal, 1*(2), 149–167.
8. Matsura, J. H. (2019). The impact of cryptocurrency on traditional currency regulations. *Civilization Law Journal, 1*(2), 123–153.
9. Moeini Far, M. (2022). Requirements for recognizing and restoring rights in digital space. *Public Law Knowledge Journal, 11*(36), 45–68.
10. Souri, P. (2022). Cryptocurrency and challenges facing legal systems. *Legal Research Journal, 2*(25), 113–142.
11. Varasi, G. (2021). Criminal policy and preventive aspects of crimes in the domain of cryptocurrencies. *Qanoon Yar Journal, 5*(19), 117–128.
12. Yazdi Nejad, A., & Dehghan, A. (2021). A blockchain EOSIO-based framework for central bank digital currency (CBDC). *Journal of Financial Knowledge and Securities Analysis (Financial Studies), 14*(50), 187–200.
13. Zarkalam, S. (2003). Electronic signature and its role in evidence law. *Modares Journal of Humanities, 7*(28), 56–87