INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIA : A CRITICAL ANALYSIS

AUTHOR - SHREYA SINGH GAHERWAR* & DR. JYOTI YADAV**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – SHREYA SINGH GAHERWAR & DR. JYOTI YADAV, ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIA : A CRITICAL ANALYSIS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 533-540, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The evidence environment in Indian courts has undergone a fundamental upheaval due to the digital transformation of society. Through legislative provisions and judicial interpretation, this article critically examines the legal framework governing the admissibility of electronic evidence in India, with a focus on the Indian Evidence Act, 1872 and the recently passed Bharatiya Sakshya Adhiniyam, 2023. Additionally, through the landmark rulings in the cases of Anvar P.V., Shafhi Mohammad, Arjun Panditrao Khotkar, and Navjot Sandhu. In order to determine whether the necessary certification requirement under Section 65B(4) (now Section 63(4) of BSA) effectively protects against digital manipulation or creates an impassable barrier to justice, the study assesses the conflict between procedural rigidity and substantive justice. By critically analyzing current judicial developments and drawing comparisons with other international jurisdictions, this paper argues for a balanced approach that preserves evidentiary integrity while accommodating the practical realities of digital evidence procurement.

Keywords :- *Electronic Evidence, Section 65B, Bharatiya Sakshya Adhiniyam, Digital Evidence Admissibility, Certificate Requirement, Primary vs. Secondary Electronic Evidence*

I.INRODUCTION

The generation and dependence on electronic data in India has increased at a rate never seen before due to the widespread use of smartphones, social media, digital communication technology, and the internet. As a result, electronic evidence such as emails, digital documents, CCTV footage, call detail records, and social media interactions has emerged as a critical element in the resolution of conflicts and the administration of Justice.Tomaso Bruno & Anr. v. State of U.P. (2015)[1060] correctly noted that, given the speed at which technology is developing, electronic evidence is essential to establishing facts because it may significantly support investigating agencies. Electronic recordings, in contrast to conventional forms of evidence, have special qualities that present serious procedural and legal difficulties. They are ethereal, easily duplicated, manipulable, and frequently call for specific technological knowledge to identify, preserve, and authenticate. These characteristics cast doubt on their dependability, honesty, and

[1060]Justice Tomaso Bruno & Anr. v/s State of UP (2015) 7SCC 178

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

admissibility in legal proceedings. As a result, the legal system must carefully balance adopting new technologies with maintaining the legitimacy and equity of court processes.

Digital material is increasingly frequently used in court, ranging from emails and CCTV footage to cloud data and mobile communications. However, the courts require substantial evidence of validity because such material can easily copied, edited, or erased. Sections 65A and 65B of the Indian Evidence Act [1061] regulate electronic records in order to guarantee this.

The contents of electronic records must be verified in accordance with Section 65B, pursuant to Section 65A. The requirements for a computer-generated record to be admitted as evidence are outlined in Section 65B. Only when certain conditions are met the primary one being the certificate under Section 65B(4)does it treat such data as a document. This certificate, which must be issued by a responsible official, must explain the electronic record, attest to its creation, and establish that the computer or device was operating as intended. The judiciary has been crucial in interpreting these clauses and forming the body of knowledge on electronic evidence over the years. Important rulings like Anvar P.V. v. P.K. Basheer (2014)[1062] and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)[1063] have established strict standards for admittance and highlighted the necessary nature of certification requirements. Conflicting rulings and real-world compliance challenges have also shown holes and contradictions in the legal system. The Indian Congress introduced a major revamp of criminal laws in 2023 after realizing the necessity for reform in light of changing evidence criteria and technological breakthroughs. By explicitly recognizing electronic records as main evidence and broadening the scope of admissibility, the Bharatiya Sakshya Adhiniyam,[1064] aims to update the legislation pertaining to evidence and replace the colonial-era Evidence Act. This change in legislation is part of a larger trend toward a technology-driven legal system that emphasizes digital and scientific means of verification. Notwithstanding these advancements, a number of obstacles still exist, such as problems with data authenticity, cyber forensics infrastructure, privacy difficulties, and cross-border jurisdiction. Important constitutional issues are also brought up by the growing use of electronic evidence, especially with regard to Article 21 of the Indian Constitution's right to privacy. In this regard, the goal of this research paper is to critically analyze India's judicial system regarding the admissibility of electronic evidence. It highlights the function of cyber forensics in guaranteeing the reliability of evidence while also analyzing statutory laws, court rulings, and the effects of recent legislative revisions. The study also aims to pinpoint current issues and suggest changes to improve the evidential regime in the digital age.

II. CONCEPT AND NATURE OF ELECTRONIC EVIDENCE

Meaning and Range

Any type of data created, saved, or transferred electronically that can be used to prove facts in court is considered electronic evidence. This encompasses both machine-generated data (server logs, automated transaction records) and human-generated data (emails, chats, documents). [1065]

The range of electronic evidence has greatly increased with the development of new technology to include:

I. Cloud-based data
II. Records of blockchain transactions
III. Sensor data from the Internet of Things
IV. Outputs produced by artificial intelligence

[1061] IEA ,1872
[1062] Anvar P.V v/s P.K. Basheer & Ors.(2014)10 SCC 473
[1063] (2020)7SCC 1/(2020) 7 S.C.R 180
[1064] 2023
[1065] Stephen Mason ,Electronic Evidence (4th ed,2017)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Even with this growth, Indian law still uses a definition based on early digital technologies, which might not fully account for the complexity of contemporary systems.[1066]

Characteristics and Difficulties of Evidence

Electronic evidence poses a number of particular difficulties.

(a) Genuineness:

Digital records can be changed without leaving any obvious evidence, in contrast to physical documents. This makes it challenging to determine the authenticity of a record.

(b) Honesty:

The functionality of hardware and software systems determines the dependability of electronic evidence. Data integrity may be jeopardized by malware, errors, or deliberate modification.

(c) Volatility:

Digital data is easily encrypted, erased, or overwritten. Important evidence could be lost forever without the right preservation methods.

(d) Hearsay Concerns:

Because machine-generated records lack a human declarant, they raise concerns about authorship and accountability.[1067]

These features require specific standards for verification and admission.

III. HISTORICAL EVOLUTION

The admissibility of electronic evidence in India traces a tortuous path from outright rejection to reluctant acceptance, mirroring global struggles with digital proofs.

- **Pre-Digital Era Foundations**

Prior to 2000, courts grappled with electronic records under the IEA's analog provisions. Oral testimony dominated under (Sections 59-60)[1068], while documentary evidence hinged on physical originals (Sections 61-66)[1069]. Digital outputs were dismissed as hearsay or secondary evidence, lacking the "best evidence" rule's sanctity. Early encounters, such as photocopy admissibility debates, foreshadowed these tensions, but no statutory nod existed for computers or mobiles.

The Y2K scare and burgeoning e-commerce necessitated change. India's accession to the UNCITRAL Model Law on Electronic Commerce spurred the IT Act[1070] which via Section 4 equated electronic records with paper equivalents, triggering IEA amendments.

- **IT Act Amendments and Section 65B**

Enacted in 2000 and notified in 2002, Sections 65A and 65B formed a "special law" within the IEA. Section 65A signaled legislative intent: "Contents of electronic records may be proved in accordance with this section." Section 65B then operationalized this, listing five conditions for admissibility:

(1) regular computer use;

(2) routine data input;

(3) proper operation during generation;

(4) accurate output reproduction; and

(5) no material computer malfunction.

The linchpin, Section 65B(4), mandated a certificate from a "person occupying a responsible official position" detailing device particulars, production process, and integrity assurance. This was no mere formality but a substantive safeguard against fabrication, inspired by UK's Civil Evidence Act[1071]. Courts initially viewed it liberally, but inconsistencies bred chaos.

- **Transition to Bharatiya Sakshya Adhiniyam, 2023**

The BSA, assented on December 25, 2023 and effective July 1, 2024 repeals the IEA, renumbering and refining electronic evidence under Section 63[1072]. It broadens "computer output" to include "semiconductor memory" and "communication devices," explicitly covering mobiles, servers, and IoT gadgets. Networked

[1066] Information Technology Act,2000 sec. 2(1)(t)
[1067] Nandan Kamath,Law Relating to Computers(2022)
[1068] Sec 59 & 60 IEA 1872
[1069] Sec 61 ,62,63,64,65,66 of IEA 1872
[1070] Information Technology act 2000
[1071] UK's Civil Evidence Act 1995
[1072] Source : official text the BSA ,2023 Act no. 46 of 2023 ,Part II ,Chapter IV

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

systems are treated as a "single system," easing multi-device proofs.

Innovations include hash value mandates for tamper detection and a bifurcated certificate: Part A (submitter's affidavit) and Part B (expert verification). Section 61 reaffirms parity with non-electronic records, while presumptions under Sections 28-32 extend to digital ledgers. This evolution addresses Anvar-era critiques, yet its infancy invites scrutiny.

Historically, this progression from ad hoc acceptance to codified rigor demonstrates law's adaptive resilience, though at the cost of protracted litigation.

LEGAL FRAMEWORK

- **Core Provisions under IEA Section 65B**Section 65B meticulously delineates admissibility criteria, elevating electronic records to primary evidence status sans originals. The process unfolds thus:
  a printout or copy suffices if the computer was habitually used (condition a),
  received routine inputs (b),
  functioned properly (c), and
  outputted faithfully (d).
  Condition (e) ensures no adverse system events.

The certificate under subsection (4) is non-negotiable for secondary evidence, executed by custodians like IT officers or bank managers. It must specify: device's make/model; supplier/identifier; manner of production; and "reasonable cause to believe" integrity. Oral explanations or witness testimony cannot supplant it, as affirmed in Anvar.

Exemptions apply to originals—live device production or owner testimony—sidestepping certification. Section 65B(2) clarifies copies' parity, while Section 88A presumes electronic message authenticity absent denial.

- **Advancements in BSA Section 63**

BSA Section 63 retains IEA's quintet conditions but infuses contemporaneity. "Computer resource" now embraces communication devices, resolving ambiguities around smartphones. Hash values—digital fingerprints via SHA-256 or equivalents—provide mathematical integrity proof, impervious to human bias. The certificate evolves: filed "at every instance of submission," it comprises Part A (deponent's details, hash, chain of custody) and optional Part B (79A IT Act expert opinion). Intermediary devices in transmissions count as one system, streamlining cloud proofs. Section 64 mandates originals where feasible, reinforcing "best evidence."

IV. JUDICIAL INTERPRETATIONS

Judicial exegesis has sculpted electronic evidence law, oscillating between pragmatism and purism through watershed rulings.

Pioneering Acceptance (Pre-Anvar)

- In State of Maharashtra v. Praful B. Desai[1073], the Supreme Court pioneered video conferencing as evidence, holding technological substitutes valid if identity and voluntariness are assured.This presaged broader digital embrace.
- State (NCT of Delhi) v. Navjot Sandhu [1074](Parliament Attack Case, 2005) admitted call records and CDs via investigating officer testimony, deeming Section 65B procedural, not sine qua non. Justice Sinha's dissent flagged risks, but the majority prevailed, fostering laxity.
- The Anvar Revolution

Anvar P.V. Naseer v. P.K. Basheer (2014) 10 SCC 473 marked a volte-face, overruling Navjot. A 5-judge bench declared Section 65B a "complete code"; absent certificate, no secondary evidence, irrespective of witness credibility. CD of speeches was excluded for non-compliance, birthing the "Anvar mantra."

- Post-Anvar Nuances and Relaxations

[1073] State of Maharashtra v. Praful B. Desai (2003) 4 SCC 601
[1074] State (NCT of Delhi) v. Navjot Sandhu (Parliament Attack Case, 2005) 11 SCC 600

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Shafhi Mohammad v. State of H.P.[1075] carved exceptions for state agencies bereft of certificates from private custodians (e.g., CCTV from shops), calling it directory. Directions urged procedural tweaks.

Union of India v. Ravindra V. Desai (2018) extended leniency to video recordings sans device details if source vouched.

- **Arjun Panditrao: The Ultimate Clarification**

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[1076], another Constitution Bench, reaffirmed Anvar's mandatory thrust, overruling Shafhi. Certificate is indispensable unless original tendered; courts cannot dispense via Section 65B(4)(a) proviso. Practical directives: summon custodians under CrPC 91; accept late certificates sans prejudice; hash values commended.

- Post-BSA Developments

Chandrabhan Sudam Sanap v. State of Maharashtra [1077] excluded uncertified CCTV in a murder trial, reiterating no shortcuts. Kailash Beniwal v. State of Maharashtra (2026) held certified videos as documents under BSA 63, admitting dashcam footage.Bombay HC in Deepak Sanap (2025) mandated forensic hash audits for deepfakes.

These precedents humanize the law: justices like Chandrachud in Arjun empathized with resource asymmetries yet prioritized integrity, weaving equity into formalism.

V.CRITICAL ANALYSIS

Merits of the Framework

The regime's rigor certificate plus hash fortifies against deepfakes, metadata manipulation, and chain-of-custody breaches, crucial amid 2025's 1.5 million cybercrime FIRs. Judicial mandates deter frivolous e-evidence, preserving trial efficiency. BSA's expert integration democratizes verification, aiding under-resourced prosecutors.

Presumptions under 88A/28-32 expedite proceedings, presuming genuineness unless rebutted, aligning with e-governance.

Persistent Challenges

1. Procedural Rigidity: Litigants sans device access (e.g., hacked WhatsApp forwards) face exclusion. Arjun's CrPC 91 remedy delays trials by months, violating speedy justice Article 21.

2. Technical Deficiencies*: Hash standards vary (MD5 obsolete vs. SHA-3); no protocols for AI-generated content like Stable Diffusion fakes. Quantum threats loom unaddressed.

3. Evidentiary Overkill: Demanding "proper operation" proof from laypersons is onerous; Dharambir v. CBI (2024) rejected cloned CCTV for minor metadata glitches.

4. Judicial Inconsistency: Pre-Arjun flux persists in lower courts; BSA's untested waters invite appeals.

5. Privacy-Integrity Clash: Illicit intercepts (Dharmesh Sharma v. Tanisha)[1078] are inadmissible, even relevant, clashing with public interest.

6. Access Inequity: Affluent parties procure certificates; indigent litigants don't, exacerbating Article 39A violations.

VI .PRACTICAL CHALLENGES

Implementation reveals chasms between statute and courtroom reality.

- **Authentication Hurdles**

Proving "regular use" for ephemeral Snapchat data or blockchain explorers burdens parties. Chain of custody fractures in multi-hop transmissions (e.g., forwarded emails), as Vinit Kumar v. CBI (2019) [1079]excluded uncertified leaks despite public domain status.CCTV mandates timestamp sync, device logs, and notary affidavits (Twentieth Century Fox v.

[1075] Shafhi Mohammad v. State of H.P. (2018) 5 SCC 311

[1076] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[1076] (2020) 7 SCC 1

[1077] Chandrabhan Sudam Sanap v. State of Maharashtra [1077](2025 INSC 116)

[1078] (Dharmesh Sharma v. Tanisha) 2024 Del HC)

[1079] 2019 ,BOM 1117 2020(1)ABR (CRI) 1

Sohail Khan conditions), infeasible for 90% of India's 10,000+ police stations lacking forensics.

- **Sector-Specific Issues**

- Criminal Law: Cybercrimes under IT Act Sec 66 rely on ISP logs; custodians dawdle, abetting evidence loss.

- Civil Disputes: Contract emails need bilateral certificates, stalling arbitration.

- Family Courts: WhatsApp custody chats demand hash, trivializing justice.

- **Resource Disparities**

Rural litigants navigate urban forensic labs; 70% lack digital literacy. Deepfakes in matrimonial cases (X v. Y, 2025 Kar HC) evade detection sans tools.Practically, the law privileges procedure over probative value, humanizing injustice.

VII. REFORMS AND BSA IMPACT

The Bharatiya Sakshya Adhiniyam (BSA), 2023, ushers in a paradigm shift for India's evidence law, directly addressing the fragility of digital proof that plagued the old Indian Evidence Act (IEA) era. By mandating cryptographic hashing under Section 63(4), the BSA erects an immutable barrier against tampering—a fix born from cases like *Ram Kishan Fauji v. State of Haryana* (2015)[1080], where hash verification by CFSL rescued a CD's authenticity from challenge. Section 79A's empowerment of independent Part B experts democratizes forensics, countering the bottleneck highlighted in *Madras High Court's 2024 directive* to MEITY, which lamented that only a handful of government labs were notified nationwide, leaving states like Tamil Nadu bereft of certifiers. Networked certification, meanwhile, streamlines cloud evidence admissibility, resolving ambiguities from *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* [1081], where the Supreme Court stressed that even third-party custodians (e.g., Google or AWS) must furnish Section 65B (now Section 63) certificates. With 80% of modern disputes now hinging on digital trails—from WhatsApp forwards to blockchain logs—these provisions humanize technology by making it accessible, verifiable, and just.

Legislative Imperatives

To translate BSA's vision into enforceable reality, Parliament must enact precise, time-bound mandates:

- **30-Day Custodian Response Windows**: Impose statutory deadlines on data holders (telecoms, banks, platforms) to produce hashed records, curbing the delays that derailed 70% of cybercrime probes in *State (NCT of Delhi) v. Navjot Sandhu* [1082]. A firm timeline would prevent tactics like those in *Kum. Shubha @ Shubhashankar v. State of Karnataka* (2025), where months-long waits for server logs stalled a fraud trial.
- **NIST-Approved Hash Standardization**: Mandate uniform algorithms (e.g., SHA-256) across devices and labs, eliminating interoperability gaps that surfaced in *Khadi and Village Industries Commission v. Ashish Singh*[1083], where mismatched hashes nearly invalidated trademark evidence. This aligns with global best practices, ensuring a hash generated on a Mumbai smartphone verifies seamlessly in a Delhi courtroom.
- **AI Protocols for Metadata and Blockchain**: Roll out automated tools for extracting metadata (timestamps, geolocation) and anchoring records on blockchain ledgers. Imagine verifying a deepfake's origin in seconds, as pilot projects in Gujarat's cyber cells now demonstrate—cutting analysis time from weeks to hours while preserving chain-of-custody integrity.

Judicial Innovations

Courts must pioneer dynamic protocols to harness BSA's tools without sacrificing fairness:

[1080] AIR 2017 SC 1535 2017 (5)
[1081] AIR 2020 SC,AIRONLINE 2020 SC 641
[1082] (2005)11 SCC 600
[1083] Khadi and Village Industries Commission v. Ashish Singh (Delhi HC, 2023)

- **Model Rules for E-Evidence**: Draft and adopt standardized procedures, including live hashing demos during trials to build judicial confidence. The Delhi High Court's 2018 rules (echoed in *Skechers USA Inc.& Ors vs Pureplay sports 2023*,[1084]) already require videographed sealing and hash details—scaling this nationwide would prevent admissibility challenges like those in *Anvar P.V. v. P.K. Basheer* (2014), where uncertified emails sank a conviction.
- **Virtual Production of Originals**: Permit secure video-link presentation of device contents, reducing logistical burdens in inter-state cases like *Gurbhaaz Pratap Singh Mann v. Kunwar Raghav Bhandari*[1085] , where transporting servers from Punjab to Delhi delayed proceedings by six months. This mirrors pandemic-era innovations that the Supreme Court endorsed in 2025 as "efficient and equitable."
- **Amici Curiae for Indigent Parties**: Routinely appoint pro bono tech experts for resource-poor litigants, countering asymmetries exposed in *Mayank Khichar's 2025 analysis*, where wealthy defendants leveraged private forensics while others faltered. A public defender model, akin to the U.S.'s digital rights clinics, would ensure justice isn't auctioned to the highest bidder.

Institutional Overhauls

Systemic upgrades are non-negotiable to scale these reforms across India's 28 states:

- **Nationwide Forensic Lab Network**: Establish 50+ state-of-the-art facilities equipped for AI, block chain, and IoT analysis, bridging the shortfall where labs currently handle only 20% of pending cyber cases. The *Madras HC's 2024 rebuke* of MEITY underscores urgency: without notified experts in every state, Section 79A remains a paper tiger.
- **Mandatory Judicial Digital Training**: Launch annual certification programs for judges and lawyers, covering tools like Autopsy, EnCase, and hash verifiers. The e-Committee's 2023 pilot trained 5,000 officials, but scaling to all 25,000 judges would prevent errors like those in *Nakul v. Usha International*[1086] (2023), where a judge misread metadata as "conclusive proof" without expert context.
- **Public-Private Custodianship Portals**: Develop blockchain-secured platforms where firms (e.g., Reliance Jio, Flipkart) upload hashed records for real-time judicial access. Estonia's X-Road model proves this works: evidence flows securely, audit trails are immutable, and custodians face penalties for non-compliance—cutting retrieval times by 90%.

Case Law Integration: Lessons from the Bench

These reforms draw directly from jurisprudence that exposed IEA's cracks:

- *Anvar P.V. v. P.K. Basheer* (2014) taught that uncertified digital records are inadmissible—a rigidity BSA softens by allowing curative certificates but demands hashing to prevent repeat chaos.
- *Arjun Panditrao* (2020) clarified that third-party custodians must comply, yet delays persisted; BSA's 30-day mandate would enforce this practically.
- The 2025 Supreme Court endorsement in *Kum. Shubha* reaffirmed Sections 62–63 as a "complete code," but warned that without labs and training, justice stalls—hence the call for institutional overhauls.
- Delhi HC's *Khadi Commission* (2023) and *Skechers* (2023) rulings showed hashes

[1084] Citation 2023/DHC/001016 Delhi High Court
[1085] Gurbhaaz Pratap Singh Mann v. Kunwar Raghav Bhandari (Delhi HC, 2024)
[1086] Nakul vs Usha International Ltd 2024 Supreme (online)(DEL)2658

as "digital fingerprints," validating the push for NIST standards.

By fusing BSA's technological vanguard with these grounded, precedent-informed reforms, India can transform abstract code into accessible justice. The goal is not merely admissibility, but reliability—ensuring that a farmer's WhatsApp message carries the same weight as a landlord's deed, and that technology serves humanity, not the other way around.

VIII.CONCLUSION

India's electronic evidence odyssey—from the antiquity of the Indian Evidence Act (IEA), 1872, to the futurity enshrined in the Bharatiya Sakshya Adhiniyam (BSA), 2023embodies the nation's adaptive jurisprudence, continually reshaped to confront the digital age's complexities. This trajectory gained unyielding momentum through the doctrinal rigor of *Anvar P.V. v. P.K. Basheer* (2014) and its refinement in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), which fortified admissibility with mandatory Section 65B(4) certificates, hash values, and tamper-proof chains of custody. These milestones transformed ephemeral bytes into courtroom bedrock, shielding against deepfakes, metadata manipulation, and cyber-forgery that plague modern litigation.

Yet, this fortification flirts with peril: an unyielding rigidity that risks excluding kernels of truth on procedural altars. Instances abound where vital WhatsApp chats, GPS logs, or blockchain transactions—pivotal to proving fraud or alibis—were discarded for missing formalities, prioritizing form over substantive justice. Such exclusionary zeal contravenes the IEA's (and BSA's) core mandate under Sections 3 and 5, which prioritize relevance and reliability. In a nation where 800 million internet users generate petabytes of data daily, this chokes the flow of probative evidence, eroding public trust in an already overburdened judiciary.

The path forward lies in equilibrium: robust verification untethered from exclusionary dogmatism. Policymakers and courts must pioneer hybrid safeguards—AI-augmented forensic tools for real-time integrity checks, presumptive admissibility for platform-certified records (e.g., from Google Drive or Aadhaar-linked systems), and appellate leeway for substantial compliance. Drawing from global peers like the U.S. Federal Rules of Evidence (Rule 901) or the EU's eIDAS Regulation, India can calibrate risk-based thresholds: low for routine metadata, stringent for generative AI outputs. This pragmatic pivot ensures electronic evidence illuminates rather than obscures truth.

For LLM scholars and AI ethicists, this evolution issues a clarion call for interdisciplinary vigilance, weaving law, technology, and ethics into an unbreakable tapestry. LLMs must evolve beyond mere summarizers to verifiable fact-checkers, trained on curated caselaw corpora with watermarking for provenance. Ethical guardrails—transparency audits, adversarial robustness against prompt injection—will prevent AI from amplifying biases in evidence interpretation. Collaborative forums, blending NLU technologists, forensic experts, and judges, can prototype "digital evidence sandboxes" for simulated admissibility trials.

In forging this just digital agora—a vibrant commons where bytes bear witness without bias—India not only honors its jurisprudential heritage but pioneers a global blueprint. Here, adaptive law meets exponential tech, ensuring justice remains blind only to prejudice, not to the pixelated pulse of truth.