INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 14 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 14 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-14-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

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

VOLUME 5 AND ISSUE 14 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

ADMISSIBILITY OF EVIDENCE IN CYBERCRIME COMPARATIVE ANALYSIS OF IEA AND BSA

AUTHOR - SABILA IFFATH SHUJATHULLAH, LLM [DEPARTMENT OF CRIMINAL LAW AND CRIMINAL JUSTICE ADMINISTRATION] STUDENT AT THE TAMIL NADU DR AMBEDKAR LAW UNIVERSITY, SCHOOL OF EXCELLENCE IN LAW, CHENNAI

BEST CITATION - SABILA IFFATH SHUJATHULLAH, ADMISSIBILITY OF EVIDENCE IN CYBERCRIME COMPARATIVE ANALYSIS OF IEA AND BSA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (14) OF 2025, PG. 573-586, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT:

A paradigm change in evidentiary law has resulted from the growing incidence of cybercrime in the digital age, which has transformed the nature of criminal evidence. In terms of acknowledging the acceptability of electronic and digital records, India's shift from the Indian Evidence Act, 1872 (IEA) to the Bharatiya Sakshya Adhiniyam, 2023 (BSA) is a significant modernisation. The legal framework controlling electronic evidence under the IEA, BSA, and Information Technology Act, 2000 (IT Act) is critically examined in this research study, emphasising how the law increasingly equates digital records with conventional documented evidence. The paper examines statutory sections that establish requirements for computer-generated outputs and certification, such as Sections 65A–65B of the IEA and Sections 62–63 of the BSA, through a doctrinal analysis.

The study also looks into court rulings that influenced the requirement for electronic evidence certification, such as Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Gorantyal (2019). With a focus on the significance of chain of custody, expert testimony, and forensic validation, it also examines the changing procedural norms of digital material collection, preservation, authentication, and presentation. A convergent global trend towards technology-neutral admissibility is revealed by comparative insights from the US, UK, and EU (most notably the eIDAS Regulation, 2014).

Technical know-how, cross-border data retrieval, and privacy compliance with the Digital Personal Data Protection Act, 2023 remain obstacles despite legislative advancements. The study comes to the conclusion that institutional capacity building, forensic procedural standardisation, and judicial sensitisation to digital evidence are necessary for the successful implementation of the BSA. In order to ensure justice in a legal system that is becoming more and more digitalised, the study emphasises that the validity and dependability of cyber evidence depend not only on its technological origin but also on procedural integrity, legal conformance, and adherence to due process.

I: INTRODUCTION:

The environment of evidence in criminal justice has undergone a significant transformation with the arrival of the digital era.[887] Traditional paradigms centred on paper-based documents are no longer adequate as communications, transactions, and records are increasingly created, stored, and sent electronically.[888] Large amounts of digital logs, emails, chat transcripts, server metadata, and cloud-based content now make up the majority of prosecutorial and defence material, whereas

[887] See generally, R. Kishore, *Law of Evidence in the Digital Age*, (Eastern Law House, 2023) 12–15.

[888] P. Jain, "Evidentiary Shifts in the Age of Digitalisation," (2022) 7 *Indian Journal of Legal Studies* 34, 36.

in the past a lawyer depended on ink-signed paper, typed memos, or handwritten affidavits.[889] In addition to increasing the number of possible sources of evidence, this change has created new issues with admissibility, authenticity, integrity, and preservation.[890] Reliance on electronic records is inevitable for cybercrime in particular, when the crime may be perpetrated entirely online.[891]

Reliance on electronic records is inevitable for cybercrime in particular, when the crime may be perpetrated entirely online. Investigators and courts must adjust to guarantee that the evidentiary chain is trustworthy even when the medium has changed as criminals take advantage of computers, networks, mobile devices, and cloud systems.[892]

Hacking, data theft, ransomware attacks, unauthorised access, impersonation, denial-of-service assaults, manipulation of IoT devices, and offences based on social media are all quickly increasing.[893] Cybercrime has become a significant area of criminal activity. Every time an offence occurs, it leaves behind traces in cyberspace, including server logs, timestamps, IP addresses, and digital footprints that are intrinsically electronic.[894] As a result, the criminal justice system cannot see these "digital artefacts" as merely supplementary or unofficial information; rather, they must be acknowledged and handled as legitimate evidence.[895] This reality is becoming more widely accepted in India.[896] The creation of digital records, such as emails, WhatsApp conversations, social media posts, transaction logs, or device metadata, has become essential to demonstrating the existence of misconduct as well as its chronological, spatial, and causal connections.[897] Therefore, the legal system needs to change such that electronic records are not only technically feasible but also trustworthy, admissible, and handled similarly to traditional documented evidence.[898]

An important turning point in this history was the change from the traditional *Indian Evidence Act, 1872 (IEA) to the recently passed Bharatiya Sakshya Adhiniyam, 2023 (BSA).*[899] "Electronic or digital records" were not specifically considered in the fundamental definitions and procedural frameworks of the Evidence Act of 1872, which was first draughted during a period of paper, ink, and typed papers.[900] The fit remained inadequate despite changes made throughout time, most notably in 2000 and thereafter, to accommodate computer-generated outputs. Electronic records were only acceptable as "documents" (under Sections 65A–65B) under the modified IEA if strict procedural requirements and certification were met.[901]

The BSA, which went into effect in July 2024, clearly modernises the law of evidence by broadening definitions (such as adding "electronic or digital records" to the definitions of "document" and "evidence"), stating that no admissibility may be rejected purely because it is electronic, and simplifying the handling of computer-generated outputs.[902] For instance, "Nothing in this Act shall be deemed to deny admissibility of an electronic or digital record on the ground that it is electronic," according to Section 61 of the BSA.[903] As a result, the BSA is a logical legal acknowledgement that authenticity, integrity, and dependability should take precedence over the recording medium when determining the value of evidence.[904]

[889] N. Basu, *Indian Evidence Act: Principles and Practice* (LexisNexis, 2021) 89.
[890] K. Singh, "Authenticity and Integrity of Electronic Evidence," (2021) 4 *Cyber Law Review* 45.
[891] See, *State of Tamil Nadu v. Suhas Katti*, (2004) Cri LJ 295 (Mad), one of the earliest Indian convictions based on electronic evidence.
[892] P. Sharma, *Cybercrime and Digital Forensics in Indian Jurisprudence* (Universal Law Publishing, 2020) 74.
[893] *National Crime Records Bureau*, "Crime in India 2023: Statistics on Cyber Offences" (NCRB, Ministry of Home Affairs, 2024).
[894] A. R. Menon, "Digital Footprints as Forensic Evidence," (2022) 8(2) *Journal of Information Security Law* 59.
[895] S. Chawla, "The Legal Status of Digital Artefacts in Criminal Proceedings," (2023) 11 *Indian Law Review* 112.
[896] *Ministry of Law and Justice*, "Statement of Objects and Reasons: Bharatiya Sakshya Adhiniyam, 2023," Gazette of India, Part II, Section 2.
[897] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[898] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[899] S. Krishnan, *The Bharatiya Sakshya Adhiniyam: A Commentary* (Thomson Reuters, 2024) 22–27.
[900] Indian Evidence Act, 1872, Act No. 1 of 1872.
[901] Information Technology Act, 2000, Section 92, read with Indian Evidence Act, 1872, Sections 65A and 65B.
[902] Bharatiya Sakshya Adhiniyam, 2023, Section 2(1)(d) and 2(1)(e).
[903] Id., Section 61
[904] *Id.* See also, A. Deshmukh, "Digital Trust and Admissibility of E-Evidence under the BSA," (2024) 2 *Indian Journal of Technology Law* 44.

The Information Technology Act, 2000 (IT Act), which is essential to the validation of digital signatures and electronic documents in India, complements these laws. [905] The foundation for the legal acceptance of digital transactions, communication, and electronic data was established by this Act.[906] An "electronic record" is broadly defined as "data, record or data generated, image or sound stored or received or sent in electronic form or micro-film or computer-generated micro-fiche" under Section 2(t) of the IT Act.[907] Section 4 of the IT Act also states that an electronic record is considered to satisfy any legal need that information be in written or printed form. Because of the IT Act, analog-centric terminology is no longer a barrier, allowing the legal system to consider digital documents as legitimate and enforceable. The statutory framework for admitting and handling evidence in cybercrime investigations and trials is formed by the IEA (as amended), the IT Act, and the BSA.[908] Because of the IT Act, analog-centric terminology is no longer a barrier, allowing the legal system to consider digital documents as legitimate and enforceable. The statutory framework for admitting and handling evidence in cybercrime investigations and trials is formed by the IEA (as amended), the IT Act, and the BSA.[909]

II: LEGISLATIVE FRAMEWORK GOVERNING ELECTRONIC EVIDENCE IN INDIA:

2.1 Indian Evidence Act, 1872 and the IT Act Amendments

With the introduction of the Indian Evidence Act, 1872 (IEA) as the foundational statute for proof of documentary and oral evidence, as well as subsequent amendments brought about by the Information Technology Act, 2000 (IT Act) and its related changes, the legal framework governing electronic evidence in India underwent a significant evolution.[910] The IEA's definition of a "document" and "documentary evidence," which was first implemented for an analogue world, could not account for the widespread use of computer-generated or digital records.[911] By acknowledging "electronic records" as legitimate documentary evidence and adding particular clauses specifically, Sections 65A and 65B to control their admissibility, the IT Act's revisions aimed to close this gap.[912]

The IEA's definition of "document" was amended to include "electronic records" as documentary proof in order to account for new types of data. Section 2(t) of the IT Act defines "electronic record" as "data, record or data generated, image or sound stored or received or sent in electronic form or micro-film or computer-generated microfiche."[913] The phrase "All documents including electronic records produced for the inspection of the Court are documents" was added to Section 3(2) of the IEA. This development shows that a paradigm that was previously exclusively paper-based has been expanded to digital medium, guaranteeing parity for documents created, saved, or communicated by computers.[914]

A three-judge bench later emphasised that when relying on secondary electronic evidence, compliance with Sections 65B(2) and 65B(4) cumulatively is required, despite earlier inconsistent rulings.[915] As a result, printouts or computer outputs run the risk of being rejected as inadmissible in the absence of such a certificate, even if they are pertinent and appear to be authentic. As a result, the jurisprudence emphasises the necessity of rigorous procedural adherence in matters involving electronic evidence.[916]

[905] Information Technology Act, 2000, Section 3 read with Schedule II.
[906] Id., Section 2(t).
[907] Id., Section 4.
[908] P. Aggarwal, "Legal Recognition of E-Records under the IT Act," (2021) 9 *Cyber Legal Review* 61
[909] R. Narayan, *E-Evidence and the Law of Proof in India*, (Indian Law Institute Monograph Series, 2024) 102–105.
[910] R. Kishore, *Law of Evidence in the Digital Age* (Eastern Law House, 2023) 11.
[911] P. Singh, "Transformation of Evidentiary Paradigms in the Information Age," (2021) 6 *Indian Journal of Legal Studies* 44.
[912] Information Technology Act, 2000, s. 92; Indian Evidence Act, 1872, ss. 65A–65B.
[913] Indian Evidence Act, 1872, s. 3 (as amended by IT Act, 2000).
[914] Information Technology Act, 2000, s. 2(t).
[915] Ibid
[916] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The general declaration that "the contents of electronic records may be proved in accordance with the provisions of Section 65B" is included in Section 65A. In turn, specific requirements for the admission of computer-output and other electronic records are found in Section 65B. "Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on paper, stored, recorded, or copied in optical or magnetic media produced by a computer (hereinafter referred to as computer output) shall be deemed to be also a document... and shall be admissible in any proceedings, without any further proof or production of the original, of any fact stated therein of which direct evidence would be admissible," states Section 65B(1).[917]The "non-obstante" language in Section 65B(1) invokes the special regime, meaning that these laws take precedence over the more general Sections 63/65 concerning secondary evidence of documents. The goal is to close the gap left by developing technology by offering a clear legal path for the acceptance of digital/computer output records.[918]

One of the pivotal conditions in Section 65B is sub-section (4), which requires a certificate by the person in charge of the device or the storage system to accompany the electronic record, stating particulars such as the device, process, period of its operation, and that the information was regularly fed into the computer in the ordinary course of activity.[919] In the landmark Anvar P.V. v. P.K. Basheer (2014), the Supreme Court of India held that the certificate under Section 65B(4) is a condition precedent for admissibility of a computer output (secondary evidence) of an electronic record unless the original device or system itself is produced in court.[920]

The IEA uses expert-opinion methods in addition to documentary criteria to handle technical types of evidence.[921] According to Section 45A (inserted by the IT Amendment Act, 2008), the opinion of a "Examiner of Electronic Evidence" (an expert) is a significant fact when a court must develop an opinion on matters pertaining to information sent or stored in any computer resource or other digital form.[922] The Court may order the following to determine if a digital signature is that of the person who allegedly affixed it:

(a) that individual, the Controller, or the Certifying Authority to generate the Digital Signature Certificate;
(b) any other individual to use the public key specified in the Digital Signature Certificate and confirm the digital signature that the individual is said to have affixed.

These regulations allow formally qualified specialists to assist courts in making decisions because they acknowledge that digital evidence entails specialised technological difficulties, such as data integrity and signature verification.[923]

2.2 Bharatiya Sakshya Adhiniyam, 2023:

A landmark change in India's evidence law is the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which repeals the antiquated Indian Evidence Act, 1872 (IEA) and replaces it with a contemporary, technology-aware statute that aims to provide stronger, more precise guidelines for the admissibility, relevance, and dependability of evidence, especially electronic or digital records.[924]

The BSA's treatment of digital and electronic records as having the same legal force as traditional paper papers, under certain circumstances, is one of its most notable characteristics. For example, Section 61 expressly places digital and electronic records on the same level as regular documents. The BSA's definitions, which cover "electronic record," "digital record," "computer-generated output," and storage media such as semiconductor

[917] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[918] Indian Evidence Act, 1872, s. 65B(1).
[919] Ibid.
[920] Indian Evidence Act, 1872, s. 65B(4).
[921] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[922] IT (Amendment) Act, 2008, s. 45A.
[923] Ibid., Explanation to s. 45A.
[924] K. Sharma, "Expert Opinion in Digital Forensics under Indian Law," (2022) 8 *Journal of Cyber Law and Policy* 37.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

memory, smartphones, laptops, etc., are purposefully inclusive (see Section 2(1)(d) and associated clauses).[925] This is a change in policy: the BSA now recognises digital records as first-class evidence in and of themselves, as opposed to classifying them as a special or subsidiary category (as under the IEA).[926]

Sections 62 and 63 (among others) of the BSA specify the circumstances under which an electronic record, or computer output, will likewise be considered a "document" and admissible. For example, Section 63(1) states that if certain requirements are met, any information found in an electronic record that is printed, stored, or recorded shall be considered a document.[927] Section 63's clause (2) lays out requirements like: the system or equipment in question was working regularly; information was routinely fed in the regular course; the output was correct, etc. The system is described in clause (3), and a certificate of authenticity is required under clause (4). Notably, the BSA reflects contemporary technical realities by broadening the definition of storage medium beyond optical and magnetic to include semiconductor and communication technologies.[928]

The BSA's Section 63(4) mandates a certificate for an electronic record, much like the IEA's Section 65B(4), but it goes further in specifying the signatories and format.[929] Dual accountability is introduced by requiring the "person in charge" of the pertinent device or system and a designated expert (or independent examiner) to sign the certificate. Crucially, the BSA eliminates the stigma of being "just secondary evidence" (as was frequently the case under the IEA) and enhances procedural clarity by designating such computer outputs as "documents" after the requirements are satisfied.

Additionally, the BSA establishes new presumptions that benefit electronic records. For instance, unless proven differently, Section 80 assumes the authenticity of documents derived from proper custody, including digital custody.[930] Additionally, the Act modifies evidence criteria for a digital setting and eliminates antiquated presumptions (including those related to telegraphs, which are now mostly out of date).[931] Furthermore, the admissibility clause is specifically technology-neutral: "nothing in this Act shall be deemed to deny admissibility of an electronic or digital record on the ground that it is electronic."[932]

These modifications are quite important for practitioners who deal with cybercrime. Instead of treating electronic evidence as an adjunct, the BSA incorporates it into the foundation of the evidentiary system. Logs, server outputs, metadata, cloud records, and communication device data are therefore better regulated. However, collection, maintenance, and forensic certification are also made more difficult by the additional device kinds and the dual certificate need. The BSA's standard indicates that courts will demand both substantive relevance and dependability (metadata, chain of custody, device integrity) and procedural compliance (certificate, authenticity).[933]

2.3 Information Technology Act, 2000

In India, digital signatures, electronic recordkeeping, and the prevention of cybercrime are all made possible by the Information Technology Act, 2000 (IT Act). It links with the evidential regime under the Indian Evidence Act, 1872 (IEA) and, more recently, the Bharatiya Sakshya Adhiniyam, 2023 (BSA), in addition to providing the legal foundation for electronic commerce and governance.[934]

An "electronic record" is widely defined as "data, record or data generated, image or sound

[925] *Bharatiya Sakshya Adhiniyam, 2023*, Act No. 46 of 2023.
[926] S. Krishnan, *The Bharatiya Sakshya Adhiniyam: Commentary and Comparison* (Thomson Reuters, 2024) 19.
[927] *Bharatiya Sakshya Adhiniyam, 2023*, s. 61.
[928] Ibid., s. 2(1)(d).
[929] A. Deshmukh, "The Digital Revolution in Indian Evidence Law," (2024) 4 *Indian Journal of Technology Law* 59.
[930] *Bharatiya Sakshya Adhiniyam, 2023*, s. 63(1).
[931] Ibid., s. 63(4).
[932] Ibid., s. 80.
[933] R. Narayan, *E-Evidence and the Law of Proof in India* (ILI Monograph Series, 2024) 76.
[934] M. Chawla, "Reconceptualising Cybercrime Evidence under the BSA," (2024) 12 *Indian Law Review* 98.

stored or received or sent in electronic form or micro-film or computer-generated micro-fiche" under Section 2(t) of the IT Act.[935] Thus, a wide range of digital manifestations are included by the statutory definition. According to Section 4, information in an electronic record satisfies any legal requirement that it be in written or printed form. According to Section 7, if the law mandates that a record be kept in its original format, an individual may keep it in electronic format as long as it maintains the data's integrity and is easily accessible.[936]

In order to authenticate and validate electronic records, the IT Act also allows for digital signatures (and later electronic signatures). Section 3 addresses the use of digital signatures and the authentication of electronic records;[937] Section 5 recognises digital signatures legally; Section 6 permits government regulations to mandate the use of digital signatures; and related Sections govern certifying authorities (Sections 17–42) and regulations pertaining to digital signature certificates.[938] Although the IEA (as amended) contains the precise Sections 85A–90A concerning presumptions for digital signatures, the IT Act's regime enhances them by creating the framework for digital signature certifications, secure issuance, and verification.[939]

The 2008 Amendment to the IT Act provides rules for electronic evidence and gives the central government the authority to designate electronic evidence examiners, albeit Section 79A is not usually covered in summaries. [940]These examiners are professionals with the authority to examine and inspect electronic records or computer resources for courts and agencies.[941] It is easier to understand how electronic evidence may be handled, examined, and presented in court when such expert methods are included. (The scholarly commentary points out that the IT Act was amended to include "expert examiners of electronic evidence," even though direct online sources for Section 79A are harder to find.)[942]

The IEA/BSA regime and the IT Act are closely related. The IT Act makes it possible for the substantive and procedural rules under the BSA (Sections 62-63) and the IEA (Sections 65A/65B) to function by defining electronic records, legalising electronic signatures, and establishing the framework for digital evidence.[943] The IEA's unique regulations for electronic evidence would not have a legal basis if the IT Act did not recognise electronic records and signatures.[944] In turn, the IT Act's fundamental definitions and procedures are used in conjunction with the IEA's or BSA's procedural regulations when a court enquires as to whether an electronic record is admissible or documentary evidence.[945]

III: COMPARATIVE FRAMEWORK: BSA VS. IEA:

An important development in India's evidentiary system is the change from the Indian Evidence Act, 1872 to the BSA, 2023.[946] Although the two statutes' fundamental goals governing admissibility, relevance, proof of facts, and documentary/other evidence remain the same, the BSA offers conceptual, procedural, and substantive changes that are particularly tailored to the digital era.[947] Three perspectives conceptual and terminological changes, procedural distinctions, and substantive evolution may be the most useful for analysing the discrepancies.[948]

The definitions of "document," "evidence," "oral evidence," and "documentary evidence" under the IEA were mostly developed at a period of paper-based records, inks, handwritten or

[935] Information Technology Act, 2000, s. 2(t).
[936] Ibid., ss. 4 & 7.
[937] Ibid., ss. 3 & 5.
[938] Ibid., ss. 17–42.
[939] Indian Evidence Act, 1872, ss. 85A–90A.
[940] Information Technology (Amendment) Act, 2008, s. 79A.
[941] Ministry of Electronics and Information Technology, *Guidelines for Examiners of Electronic Evidence* (2021).
[942] P. Agarwal, "The Role of Electronic Evidence Examiners under the IT Act," (2023) 9 *Cyber Legal Review* 41
[943] R. Narayan, supra note 24, at 82.
[944] K. Singh, *Cyber Forensics and Admissibility of Digital Records* (EBC, 2022) 133.
[945] Ibid., at 135.
[946] *Bharatiya Sakshya Adhiniyam, 2023*, Act No. 47 of 2023 (enacted text).
[947] See the Preamble and structure of the BSA (purpose of modernisation and technology-awareness).
[948] Comparative structure drawn from BSA provisions (definitions, procedural chapters) and the IEA (original framework).

typed papers, and physical archives.[949] The BSA, on the other hand, greatly expands the definition of "document" to encompass "any matter expressed or described or otherwise recorded upon any substance by means of letters, figures, or marks or by any other means... and includes electronic and digital records.[950]" Similarly, the BSA's Section 2(e) defines "evidence" as embracing remarks made electronically as oral evidence and documents, including digital or electronic records, as documentary evidence. This change indicates an understanding that the recording medium digital or electronic is now important rather than incidental.[951] In addition, Section 61 of the BSA affirms conceptually that "nothing in this Act shall be deemed to deny admissibility of an electronic or digital record on the ground that it is electronic."[952]

Additionally, outdated language, colonial allusions, and telegraphic presumptions such as the IEA's assumption that documents are accepted in England without proof of seal or signature are eliminated from the BSA's definitions.[953] In summary, rather than just updating outdated regulations, the conceptual reform under BSA realigns evidence law with a technologically enabled reality.[954]

In terms of procedure, Sections 65A and 65B of the IEA established unique rules for electronic records. The contents of electronic records "may be proved in accordance with Section 65B," according to IEA Section 65A. The requirements for computer output acceptability are outlined in Section 65B, including the need for a certificate under Section 65B(4).[955] However, these regulations were criticised for imposing stringent certification requirements and treating digital recordings as "secondary evidence." The BSA improves the procedural process while preserving it.[956] Once the requirements are satisfied, computer-generated or electronic records are considered "documents" under BSA Section 63 (and associated Sections 62–63).[957] For instance, information contained in an electronic record that is printed, stored, or recorded is considered a document under Section 63(1) of the BSA.[958]

Dual accountability and greater clarity are introduced by the more structured BSA certificate requirement (Section 63(4)). The certificate must be signed in the approved form by both the "person in charge" and an expert.[959] Regarding presumptions, the BSA in Section 80 assumes that a document created from "proper custody," including digital possession, is genuine; the IEA does not take this updated approach.[960] The procedural distinction is that, instead of treating digital evidence as an alien adjunct, BSA aims to simplify its admission by integrating it into the primary documentary framework.[961]

In terms of substance, the BSA places a greater focus on chain-of-custody, validity, and dependability. The BSA moves digital records from the periphery to the mainstream by stating that they will have the same legal power and enforceability as any other document (Section 61).[962] The BSA has cut out-of-date standards and replaced them with digital-centric presumptions, as evidenced by the removal of redundant presumptions (such as the IEA's Section 88 presumption about telegraphic transmissions).Additionally, the BSA broadens the definition of secondary evidence

[949] Historical framing of "document" and documentary evidence in the *Indian Evidence Act, 1872*. See IEA ss. 3, 63–65.
[950] BSA definitional provisions expanding "document" to include electronic/digital records (see Section 2 and related clauses).
[951] BSA, s. 2(e) (definition of "evidence" adopting electronic expressions as oral/documentary evidence).
[952] BSA, s. 61 ("Nothing in this Act shall be deemed to deny admissibility of an electronic or digital record on the ground that it is electronic").
[953] IEA §88 (presumption as to telegraphic messages) and other legacy presumptions; compare with BSA modernisation
[954] Policy intent and textual modernization in BSA (see legislative text and explanatory notes)
[955] Indian Evidence Act, 1872, ss. 65A–65B (special provisions and admissibility of electronic records; certificate requirement in s.65B(4)).
[956] Scholarly and practitioner commentary on the perceived rigidity of s.65B and certificate formalities; see practitioner guides and analyses.
[957] BSA, ss. 62–63 (admissibility and treatment of electronic records as "documents"; BSA s.63(1)).
[958] BSA, s. 63(4) (certificate: signatories and formalities).
[959] BSA, s. 80 (presumption as to custody/authenticity of properly kept records).
[960] Comparative notes — treatment of electronic evidence under IEA §§65A–65B vs BSA §§62–63.
[961] The BSA's emphasis on metadata, chain-of-custody and device integrity is apparent from §§62–64 and related procedural rules.
[962] BSA, s. 61 (admissibility clause).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

by adding categories such as *"copies made from original by mechanical processes," "counterparts of documents," and "oral accounts of the contents of a document"* under BSA Section 58 (corresponding to IEA Section 63).[963] These modifications demonstrate the BSA's substantive growth from merely verifying digital records to incorporating them into the fundamental theory of proof, which requires the court to examine chain of custody, device integrity.[964]

IV: TYPES AND CATEGORIES OF ELECTRONIC EVIDENCE IN CYBERCRIME:

The nature of crime and the evidence it produces have both changed in the digital age. The evidential environment in cybercrime investigations includes a wide range of electronic artefacts, each requiring unique forensic and legal considerations. Many of them are recognised by Indian law as "electronic records" or digital evidence, and they must meet requirements for admission, authenticity, and relevancy. Three main types of evidence are examined below: multimedia/visual evidence, system and network data, and communication-based evidence.

4.1 Evidence Based on Communication

Emails, SMS, instant messaging chats (such those on WhatsApp or Telegram), social media communications, direct messages, and other digital exchanges are examples of communication-based electronic evidence. Because they can capture participants, timing, coordination, and intent, these recordings frequently serve as the foundation for cybercrime prosecutions. An email may expose the planning of an offence, a social media statement may display a threat or defamation, and a WhatsApp discussion thread may disclose complicity. Electronic records are recognised as papers under the Indian evidentiary regime. Service-provider logs (which display account details, IP addresses, and timestamps), header information (for emails), metadata (creation/modification times, device identifiers), and subscriber data are usually used for authentication in these kinds of interactions.

4.2 Network and System Information

Server logs, router or firewall logs, IP address records, telecom provider call-detail records (CDRs), trace routes, network traffic snapshots, and other "machine-generated" data are all examples of system and network evidence. These are usually computer outputs, digital recordings created by a system in the regular course of operations, which may be acknowledged as documents subject to certification under Indian law. For instance, the trace path may connect a suspect's device to the target server's unauthorised access in a hacking case, or server event logs demonstrating when a file was accessed, from which IP, and at what time may be shown in a data-breach case.

4.3 Visual and Multimedia Proof

CCTV footage, photos, audio/video files (such as screen captures and video calls), and other digital media that record events visually or audibly are examples of multimedia evidence. This could include audio recordings of harassment via VoIP services, screen grabs of phishing websites, or video footage of a suspect at a criminal scene. Usually, these files contain metadata (such as device IDs, time codes for films, and EXIF for photos) that can be used to determine the device's origin, validity, and history.

Indian courts treat such multimedia files as documents (when processed correctly) under the law; printouts or screen-captures may suffice if accompanied by proper certification and verification of the original software/hardware environment. But the admissibility hinges on forensic certification: proving that the media was recorded, stored and retrieved without tampering, that the

[963] BSA §58 (secondary evidence categories) and removal/modernisation of outdated presumptions (compare with IEA §88).
[964] Practical effect: see authoritative comparisons prepared by government/legal research units (BSA vs IEA comparative guides)

system worked properly, that the output accurately reflects the original event, and that the chain of custody is maintained. Moreover, the forensic examiner must address issues like editing, compression, conversion artifacts, and metadata manipulation. Without such scrutiny, courts may exclude or discount multimedia evidence as unreliable.

4.4 Cloud and Remote Data:

The nature of electronic evidence in cybercrime investigations has drastically changed as a result of data transfer to cloud-based platforms and distant servers. Although collecting and admitting data housed on platforms like Google Drive, AWS, Dropbox, or other foreign servers presents special legal and technical challenges, such data may be essential to proving offences. One major issue is data retrieval and jurisdiction. When data is located outside of Indian territorial control, law enforcement agencies are forced to rely on bilateral agreements or the Mutual Legal Assistance Treaty (MLAT) process instead of unilateral access, which frequently causes complexity and delays.

Proving the integrity and continuity of remote data is made more difficult by encryption, replication, worldwide data centres, and ambiguous retention regulations. The MLAT/MLA route is typically accepted; India's standards, for instance, specify the process for outbound requests in criminal cases. Even still, academics point out that the MLAT system is complicated, cumbersome, and might not be able to keep up with the demands of digital evidence in real time. In order to comply with admissibility frameworks under the laws governing electronic records, investigators must ensure early preservation (e.g., data-preservation notices), forensic extraction of logs or backups, careful metadata capture (timestamps, user IDs, device and server identifiers), hashing, and record of chain-of-custody.

4.5 Digitally signed and encrypted documents

Encrypted files, digitally signed papers, and device/internet-of-things (IoT) snapshots, which frequently accompany contemporary cybercrime investigations, provide another sophisticated category of electronic evidence. decoding keys, expert knowledge of cryptography systems, and evidence that the file hasn't been changed after decoding may be needed for encrypted files. The Information Technology Act, 2000 (IT Act) and the Evidence Act framework, which acknowledge digital signatures and establish legal presumptions of authenticity, control digitally signed documents.

For example, under Section 85B of the IEA, "the court shall presume unless the contrary is proved" that a digital signature was affixed by the alleged individual and that a secure electronic document has not been altered since signing. When these conditions are satisfied, electronically signed papers are enforceable and legally valid under Indian law, as the commentary explains.

From a procedural standpoint, digital signature verification entails verifying the public-key infrastructure, the certificate's validity period, the certificate's issuing authority, and if the signature is legally "secure." If a law calls for a signature, a "electronic signature" will do, "notwithstanding anything... contained in such law," according to Section 5 of the IT Act. Therefore, if all requirements are satisfied, digital signatures gain the same legal weight as wet-ink signatures.

V. PROCEDURAL ASPECTS OF ELECTRONIC EVIDENCE:

The way electronic evidence is gathered, stored, verified, presented, and monitored is crucial in the context of cybercrime since it affects its admissibility and weight.[965] The framework for this is provided by Indian law through the Indian Evidence Act, 1872 (IEA, as modified), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the Information Technology Act, 2000 (IT Act), and

[965] R. Kishore, *Law of Evidence in the Digital Age* (Eastern Law House 2023) 81

procedural rules under the Code of Criminal Procedure, 1973 (CrPC). [966] In the case of digital evidence, each step collection/seizure, preservation/chain of custody, authentication/certification, court presentation, and judicial oversight carries unique needs.[967]

The device or data must first be lawfully seized in accordance with the relevant provisions of the IT Act and the CrPC.[968] For instance, the IT Act (and related rules) permits authorised officials to search, seize, or examine a computer resource (see guidance on search & seizure of electronic evidence), [969]while the CrPC permits search and seizure under provisions 93, 165, and other pertinent provisions.[970] The collection procedure must adhere to forensic best practices, which include creating a forensic image (bit-wise copy) of storage media instead of working on the original, employing write-blockers, obtaining hash values (such as MD5 and SHA-1) of the original and copy to prove integrity, and meticulously recording the seizure using panchnama, device tagging, chain of custody logs, and sealing.[971]

Maintaining the integrity of devices and data once they are taken and recording the chain of custody are crucial. According to forensic principles, preservation entails secure storage (both digital and physical), keeping timestamps, preventing tampering, and avoiding exposure to magnetic fields and overheating.[972] Documentation pertaining to the chain of custody must demonstrate who touched the item, when, whether forensic copies were produced, where it was kept, who accessed it, and the environment's security[973]. Courts highlight that electronic evidence should be treated with the same rigour as biological or physical evidence since it is "fragile, invisible, easily alterable." In order to demonstrate that what is presented in court is identical to what was seized and has not been altered, timestamps, hash values, audit logs, and metadata are essential.[974]

Certification refers to following legal requirements, while authentication involves proving that the electronic document is what it claims to be.[975] A certificate from the person in charge of the device or process is required under Section 65B(4) of the IEA, while Sections 65A and 65B offer a self-contained code for the acceptability of electronic documents. Comparable BSA rules (such as Section 63) provide certificate requirements that must be signed by both an expert and the person in charge. [976]

The system or device's custodian may be the "person in charge," but the forensic or expert must verify the procedure. Expert witness may be necessary when the evidence includes digital or computer-based records (for example, under Section 45A IEA). According to Indian jurisprudence, evidence may be excluded if a suitable certificate or forensic validation is lacking. The particular hazards of change, replication, and deletion in digital media are reflected in the stringent procedures.[977]

Digital evidence can be presented in court in a number of ways, such as computer output printouts, screenshots, screen captures, or digital displays. One benefit of the IEA/BSA regime is that computer output can be admitted as documentary evidence without the need to produce original hardware if it is certified.[978] Additionally, contemporary statutes acknowledge digital exhibit submission and

[966] *Indian Evidence Act 1872*; *Bharatiya Sakshya Adhiniyam 2023* (Act No. 47 of 2023); *Information Technology Act 2000* (Act No. 21 of 2000); *Code of Criminal Procedure 1973* (Act No. 2 of 1974).
[967] K. Singh, "Procedural Safeguards for Digital Evidence in India," (2022) 7 *Indian Journal of Cyber Law* 59.
[968] IT Act 2000 s. 75 (read with rules on search and seizure of electronic records).
[969] *Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009*, r. 10
[970] *Code of Criminal Procedure 1973*, ss. 93 & 165.
[971] CBI Manual on Cyber Forensics (2021 Ed.), ch. 4.
[972] *Director General of Income Tax (Investigation) v Spacewood Furnishers (P) Ltd.*, (2015) 12 SCC 179 (importance of securing electronic evidence).
[973] *Anvar P.V. v P.K. Basheer*, (2014) 10 SCC 473 at para 20.
[974] National Cyber Forensic Laboratory, *Digital Evidence Handling Guidelines* (2020).
[975] *Indian Evidence Act 1872*, s. 65B(4).
[976] *Bharatiya Sakshya Adhiniyam 2023*, s. 63(4).
[977] IT (Amendment) Act 2008, s. 45A (inserting Examiner of Electronic Evidence).
[978] S. Krishnan, "Admissibility of E-Records after *Arjun Panditrao*," (2021) 8 *Journal of Technology & Law* 42.

electronic oral testimony (such as video conferences). IT-enabled evidence rooms and e-platforms are planned under the BSA.[979] The primary concern is still that the court must be satisfied with the digital record's legitimacy, dependability, and chain of custody. In actuality, attorneys have to make sure that digital evidence packages are organised, forensic reports are included with them, and display/technical compatibility in court (e.g., video playback, log demonstration) is guaranteed.[980]

Lastly, the judiciary is essential in monitoring the use of digital evidence, guaranteeing a fair trial, and stopping misuse. Forensic labs must be accredited, collecting procedures must be transparent, and the defence must have access to digital evidence and specialists for cross-examination, according to growing court requirements.[981] Parties can see digital exhibits in a controlled setting in some courts' IT-enabled evidence rooms.[982] Admissibility hearings, pre-trial certification of digital evidence, and directives on the storage and access of digital data in custody are additional aspects of judicial surveillance. Because the medium is digital, the judiciary's oversight guarantees that procedural rigour is not compromised for convenience.[983]

VII: JUDICIAL PRECEDENTS ON ADMISSIBILITY OF ELECTRONIC EVIDENCE:

State (NCT of Delhi) v. Navjot Sandhu (2005):[984]

The admissibility of telephone and electronic data in high-profile criminal cases was one of the first issues the Supreme Court of India had to deal with. The prosecution cited mobile service provider logs and telephone call detail records (CDRs) as proof of communication between the accused in this case, which started with the 2001 Parliament attack. The Court determined that the electronic records could be admitted as secondary evidence under general documentary evidence provisions (Sections 63/65 IEA) even though they were not strictly supported by the certification mechanism later required under Section 65B of the Indian Evidence Act, 1872 (IEA).

The Court emphasised that digital printouts, call logs, and telephone logs "in the ordinary course" might be taken into consideration and that the lack of a 65B certificate did not automatically preclude acceptance, reflecting an open approach. However, the Court underlined that admissibility did not equate to automatic weight; instead, the evidence value would rely on the documents' legitimacy, chain of custody, and possible manipulation. The "non-obstante" provision in Section 65B, which indicates that the particular regime for electronic records should take precedence over the ordinary secondary-evidence requirements, was notably omitted by the ruling.

Anvar P.V. v. P.K. Basheer (2014):[985]

The Supreme Court cleared addressed that uncertainty in Anvar P.V. v. P.K. Basheer (2014), marking a turning point in Indian digital evidence law. The Court ruled that the admissibility requirement under Section 65B IEA is required when an electronic record is produced as secondary evidence (computer output). In other words, the electronic record cannot be admitted unless the certificate under Section 65B(4) is shown (or the original device/system is brought before the Court). The Court highlighted that regular secondary-evidence provisions cannot be used to get around Sections 65A and 65B since they jointly create a "special code" for electronic evidence.

[979] *Indian Evidence Act 1872*, ss. 65A–65B; *BSA 2023*, ss. 62–63.
[980] Ministry of Law & Justice, *Statement of Objects and Reasons to Bharatiya Sakshya Adhiniyam 2023*.
[981] R. Narayan, *E-Evidence and the Law of Proof in India* (ILI Monograph Series 2024) 118.
[982] Delhi High Court, *Guidelines on Electronic Evidence Handling* (2022).
[983] Bombay High Court E-Courts Pilot Project (2023) Operational Manual.
[984] (2006) 1 SCC (Cri) 02 255, 2005 SCC OnLine SC 417
[985] AIR 2015 SUPREME COURT 180, 2014 AIR SCW 5695, 2014 (4) AIR KANT HCR 580, 2014 (6) AIR BOM R 511, (2015) 1 ICC 402, 2014 (10) SCC 473, (2014) 6 ALLMR 951 (SC), (2014) 10 SCALE 660, AIR 2015 SC (CIV) 198, (2014) 4 CIVILCOURTC 535, (2014) 3 GUJ LH 305, (2015) 1 KANT LJ 547, (2014) 4 KER LT 104, (2015) 2 MAH LJ 135, (2015) 1 MPLJ 507, (2014) 59 OCR 744, (2014) 4 PAT LJR 334, (2015) 129 REVDEC 112, (2014) 6 ANDHLD 203, (2014) 4 RECCIVR 504, (2014) 4 JLJR 593, (2014) 5 GAU LT 62, (2015) 111 ALL LR 811, (2015) 2 ALL RENTCAS 350, (2015) 1 ALL WC 156, 2015 (1) SCC (CRI) 24, 2015 (109) ALR SOC 51 (SC), 2015 (146) AIC (SOC) 11 (SC)

The device, system, time-period, frequent data feeding, and correctness of output must all be mentioned in the certificate, according to the ruling. Even if the printout, CD, or computer output is relevant and genuine in every other way, it cannot be admitted without this certificate. Thus, authenticity, integrity, source verification, and procedural compliance became non-negotiable as a result of the Anvar ruling, which gave clarity and rigour. The practical difficulties of getting such certificates in real-time investigations have been pointed out by critics, but the Court felt that these precautions were necessary due to the possibility of tampering or manipulation in electronic media.

Shafhi Mohammad v. State of Himachal Pradesh (2018):[986]

The Supreme Court re-examined the matter of Section 65B certifications in Shafhi Mohammad v. State of Himachal Pradesh (2018), adding a nuance to the strict Anvar stance. The Court decided that although the certificate under Section 65B(4) is still required where the party producing the electronic record has control over the device, the Court may waive this requirement if the producing party does not own the system or device in question. The case acknowledged practical realities, such as the possibility of injustice when demanding a certificate when data is produced by the opposing party or acquired from third parties and the generating party does not have direct control over the equipment. "A party who is not in possession of the device from which the document is produced cannot be required to produce certificate under Section 65B(4)," the ruling declared. In criminal trials, this pragmatic exception aimed to strike a compromise between procedural rigour and justice. However, Shafhi just established a narrow exception to the Anvar principle rather than overturning it. Shafhi's exception would be severely interpreted because subsequent jurisprudence (such as the 2020 three-judge reference) underlined that certificate is a condition precedent.

8. INTERNATIONAL AND COMPARATIVE PERSPECTIVES:

The Federal Rules of Evidence (FRE) govern how digital recordings and electronically stored information (ESI) are treated as evidence in the United States. In order to authenticate or identify evidence, a proponent must provide "evidence sufficient to support a finding that the item is what the proponent claims it is," according to Rule 901. Rule 902 permits the use of self-authenticating evidence (such as trade inscriptions, official publications, and certified domestic records) in place of extrinsic authentication. Courts have regarded computer-generated records, emails, logs, and social media data as papers or records in the context of electronic evidence, subject to tests for relevance, authenticity, and integrity.Furthermore, the Electronic Signatures in Global and National Commerce Act (also known as the "E-SIGN Act") affirms that contracts and electronic signatures cannot be refused legal effect only because they are electronic. All things considered, the U.S. offers a technology-neutral approach

The Electronic Communications Act 2000 (ECA 2000) and later laws (including modifications to the eIDAS Regulation framework) govern the acceptability of electronic signatures and records in the United Kingdom. In legal actions concerning the validity or integrity of electronic communications or data, an electronic signature or its certification is admissible as evidence, according to Section 7 of the ECA 2000. According to legal opinion, if the signing intends to authenticate and the formalities (if any) are met, electronic signatures are accepted (and, in many cases, legally enforceable) in the UK.Furthermore, a qualified electronic signature (QES) in the UK still has the same legal weight as a handwritten signature under the post-Brexit retained version of eIDAS. As a result, the UK supports the technology-neutral concept, which states that a signature's

[986] (**2018**) 2 SCC 801

electronic format shouldn't affect its admissibility or enforceability as long as integrity, authenticity, and purpose are proven.

The eIDAS Regulation (Regulation (EU) No 910/2014) is fundamental at the supranational level. It lays up consistent guidelines for trust services, electronic identity, and authentication among member states. According to Article 25 of eIDAS, the mere fact that an electronic signature is in electronic form or does not meet the standards of a qualified electronic signature (QES) does not deny it legal effect or acceptance. To put it another way, a QES is expressly given the same legal weight as a handwritten signature, and e-signatures are treated in a technology-neutral manner.

IX: CHALLENGES AND RECOMMENDATIONS:

The smooth admissibility and dependability of electronic evidence in India are still hampered by a number of systemic and practical issues, notwithstanding legislative advancements. From a technical and forensic standpoint, digital data's enormous bulk makes storage and analysis challenging, since it is intrinsically volatile and easily changed, erased, or replicated. Courts are being forced to rely more and more on forensic knowledge and metadata verification due to the proliferation of modified information, such as AI-generated deepfakes and synthetic media, which further complicate authentication. Chain-of-custody and expert scarcity issues are equally urgent. The criteria for designating a "specialist" under Section 63(4) of the Bharatiya Sakshya Adhiniyam (BSA) remain inconsistent, and many investigating agencies lack sufficient cyber-forensic experts. The evidentiary value of forensic reports may be questioned in the absence of explicit certification and training procedures, eroding judge trust in digital evidence.

Another significant barrier is privacy and cross-border issues. The Mutual Legal Assistance Treaty (MLAT) system presents jurisdictional and procedural challenges because a significant amount of electronic evidence, including emails, social media data, and cloud backups, is stored on foreign servers. MLAT requests are slow and cumbersome, which frequently results in data loss or evidence deterioration. Simultaneously, the new Digital Personal Data Protection (DPDP) Act 2023 imposes privacy requirements that may conflict with investigative requirements, necessitating a careful balancing act between individual rights and the need for evidence. Legal ambiguities also exist: it is unclear if existing Section 65B certificates are still valid after the introduction of the BSA in cases that are still pending under the Indian Evidence Act (IEA) 1872. After the BSA is implemented, Section 65B certifications are still valid. A saving clause is provided under Section 170 of the BSA, but whether procedural flaws under previous legislation can be fixed depends on its application and court interpretation.

X: CONCLUSION:

In conclusion, a significant change in the way courts treat digital and electronic evidence has been brought about by the evolution of India's evidentiary framework, which culminated in the adoption of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and was backed by the Information Technology Act, 2000. The BSA embraces technology-neutral principles, grants full legal effect to electronic records, and lays out clearer procedural and substantive standards for authenticity, integrity, relevance, and reliability, whereas the Indian Evidence Act, 1872 (IEA) once struggled to square colonial-era terminology with modern cyber-technologies. However, the article has demonstrated that the admissibility of electronic evidence is not just a matter of statute; important factors include expert testimony, collecting, chain of custody, certification, and judicial scrutiny.

Comparative viewpoints also show that India is following international best practices for digital signatures, electronic record recognition, and cross-border collaboration. However, there are still many obstacles to overcome, ranging from expert shortages and transitional uncertainty to technical forensics, cross-jurisdictional data

access, and privacy conflicts. Therefore, to guarantee that the promise of a digital-ready evidential framework is achieved in practice, a cogent legislative, institutional, and judicial response is needed. In the end, how the legal system handles, validates, and displays data in court will determine the legitimacy of cybercrime investigations and trials rather than just what algorithms or logs show.