

**ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIA: A
COMPARATIVE JURISPRUDENTIAL STUDY OF THE IEA, 1872 AND
THE BSA, 2023**

Shashwat Prashar¹

ABSTRACT

Introduction of digital communications has completely transformed criminal and civil proceedings, wherein the digital information has become an indispensable document of proof instead of being an additional one. It had been for almost two decades that the admissibility of such digital information had been governed in India under a statutory scheme contained in Section 65A and 65B of the Indian Evidence Act (IEA), 1872. Such a statutory scheme, which had very strict procedural pre-requisites, had evolved on the basis of a series of important judicial precedents, including the landmark cases of Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal. This paper discusses the legal doctrine of the past statute in the light of the current statutory scheme contained in Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam (BSA), 2023. The BSA, while providing forward-thinking definitions of the technology like cloud computing, smartphones, Internet of Things, and semiconductor memories, has modified the traditional concept of primary and secondary evidence, where electronic documents are considered to be primary evidence. The key, and somewhat paradoxical, finding of this paper is that the BSA does not weaken procedural formality but rather shifts it. A careful analysis of section 63(4) reveals that the level of formality required for the process of authentication of evidence in the BSA is higher than in its predecessor: Section 63(4) provides for a two-stage signature by both the individual in control of the device and the technical expert, in contrast to one signature under Section 65B(4).

Keywords: Electronic Evidence; Bharatiya Sakshya Adhiniyam, 2023; Admissibility of Digital Evidence; Authentication of Electronic Records; Section 63 BSA

¹ Shashwat Prashar, 2nd Year Law Student L.L.B (Hons), Chanakya National Law University, Patna

I. INTRODUCTION

The rapid advent of the digital age has revolutionized the methods of collecting, creation and exchange of evidences in courts. People interact with each other mostly via technology, and the law of evidence needs to change accordingly. Collecting and evaluation of evidence have been based on oral and documentary evidence; nowadays courts need to deal with emails, digital documents, and social media.

For example, the introduction of electronic evidence in India was introduced through the amendment to the Indian Evidence Act, 1872 under the Information Technology Act, 2000 where sections 65A² and 65B³ were inserted. These two sections have brought about a unique way of admission of electronic evidences that can be considered as a different class of evidences. Indeed, as a matter of fact, the provisions have been subject to much controversy over the manner in which the electronic evidence ought to be admitted especially when taking into consideration the certification provision in Section 65B(4). Important cases like *Anvar P.V. v. P.K. Basheer*⁴ and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*⁵ were some of the efforts made to clear the confusion surrounding these issues.

The Bharatiya Sakshya Adhiniyam, 2023 has been passed by Parliament with an intention to change the evidentiary laws from those that are colonial to one that can address the current technological reality. This statute commenced operation on 1 July 2024⁶ and will replace the Indian Evidence Act.

II. RESEARCH OBJECTIVES

This study undertakes a critical assessment of the evolving law governing electronic evidence in India. Its objectives are to:

- a. Identify the legal provisions relating to electronic evidence under the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023;

² Indian Evidence Act, 1872, ss. 65A, 65B (inserted by the Information Technology Act, 2000, s. 92 and Second Schedule, w.e.f. 17 October 2000).

³ Indian Evidence Act, 1872, s. 65B(4)

⁴ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473

⁵ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

⁶ Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 1(2); the substantive provisions, including ss. 61–63, came into force on 1 July 2024.

- b. Evaluate the changes introduced by the Bharatiya Sakshya Adhiniyam, particularly with respect to admissibility standards and certification requirements;
- c. Examine judicial interpretation of electronic evidence, with particular reference to *Anvar P.V. v. P.K. Basheer*⁷ and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*⁸;
- d. Identify the practical and institutional challenges affecting the admissibility of electronic evidence under both regimes; and
- e. Assess, comparatively, whether the new law genuinely relaxes procedural formalism or merely redistributes it.

III. RESEARCH QUESTIONS

- a. What were the legal standards governing the admissibility of electronic evidence under the Indian Evidence Act, 1872?
- b. How has the Bharatiya Sakshya Adhiniyam, 2023 restructured these standards, and in what respects, if any, has it relaxed them?
- c. Is the certification requirement under Section 63(4) of the BSA more, less, or comparably demanding than Section 65B(4) of the IEA?
- d. Does the Bharatiya Sakshya Adhiniyam resolve the institutional and interpretive difficulties observed under the earlier framework, or does it introduce new ones?

IV. LITERATURE REVIEW

The issue of electronic evidence being admissible has been extensively researched and decided upon in India, due to the issues caused by fast-paced technological changes. Studies on the Indian Evidence Act, 1872 have considered Sections 65A⁹ and 65B¹⁰ extensively, especially the certificate requirement in Section 65B(4). The highly cited early study by Vaidialingam pointed out that the Supreme Court's interpretation of Section 65B(4) in *Anvar P.V. v. P.K. Basheer* deviates from standard interpretations of

⁷*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

⁸*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

⁹ Indian Evidence Act, 1872, ss. 65A, 65B

¹⁰ Indian Evidence Act, 1872, ss. 65B

statutes by taking the certificate to be the sole means of authenticating the document, despite there being nothing in the language of Section 65B(4) that would limit the mode of authentication to that method alone.¹¹ The subsequent empirical survey carried out by Singh and Bamb of practices after 2014 revealed how the inconsistency finally came to rest in Arjun Panditrao Khotkar¹².

V. CONCEPTUAL FRAMEWORK: DEFINING ELECTRONIC EVIDENCE

Before assessing admissibility, it is necessary to identify what qualifies as electronic evidence as a matter of statutory definition, since the term is treated differently across the two regimes under study. The Information Technology Act, 2000 defines 'electronic record' to include data, record, image, or sound generated, stored, received, or sent in electronic form¹³. The Indian Evidence Act incorporates this definition by reference within its account of 'document' under Section 3¹⁴, without independently defining the term. The Bharatiya Sakshya Adhiniyam, by contrast, defines 'document' under Section 2(1)(d) to expressly include electronic and digital records¹⁵, and defines 'evidence' under Section 2(1)(e) to extend to facts established through electronic or digital means¹⁶. This shift from incorporation by cross-reference to an autonomous, technology-inclusive definition is a structural change in its own right, distinct from the certification question examined later in this paper. It is first required that one understands what electronic evidence means in terms of statutory language, since the two systems being considered use different understandings of the concept.

As per Information Technology Act, 2000, "electronic record" shall mean "data, record, image or sound generated, stored, received or sent in electronic form." In the Indian Evidence Act, this definition forms part of the definition of the word 'document' in section 3. On the other hand, the Bharatiya Sakshya Adhiniyam defines the word 'document' as that which contains electronic and digital document in section 2(1)(d),

¹¹ Ashwini Vaidialingam, 'Authenticating Electronic Evidence: Section 65B, Indian Evidence Act, 1872' (2015) 8 NUJS Law Review 43

¹² Bhavyakirti Singh & Aditya Bamb, 'The Dichotomy of the 65B Certificate: Analysing Trends with Regard to the Authentication of Electronic Evidence in India' (2021) 10(1) Christ University Law Journal 73.

¹³ Information Technology Act, 2000, s. 2(1)(t).

¹⁴ Indian Evidence Act, 1872, s. 3 (definition of 'document', as amended by the Information Technology Act, 2000).

¹⁵ Bharatiya Sakshya Adhiniyam, 2023, s. 2(1)(d).

¹⁶ Bharatiya Sakshya Adhiniyam, 2023, s. 2(1)(e).

while the word ‘evidence’ is defined as that which contains facts proved by electronic and digital means in section 2(1)(e). This difference in the approach towards these definitions is important as such.

The additional issue of definition relates to classification. In general terms, electronic evidence encompasses e-mail and other messaging transactions, digitalized documentation, voice and video recordings, metadata, network communication, cloud-based data storage, and semiconductor memory-based data storage.¹⁷ Within this wide class of electronic evidence arises an issue of taxonomy for both statutes to grapple with; namely, whether an electronic record constitutes primary or secondary evidence as a matter of its nature. In India, electronic records generated as “computer output” constituted a subset of secondary evidence which could be proved by means of the specific procedure under Section 65A and 65B of the Indian Evidence Act rather than under the general provisions relating to primary and secondary evidence.¹⁸

VI. ADMISSIBILITY UNDER THE INDIAN EVIDENCE ACT: A DOCTRINAL HISTORY

Sections 65A and 65B were added to the Indian Evidence Act through the Information Technology Act, 2000, which came into force on 17 October 2000¹⁹. The section 65A states that electronic records can be proved in accordance with section 65B²⁰, where a ‘computer output’ is considered to be a document that is admissible without any additional proof of the original, subject to the provisions of Section 65B(2) and where there is a certificate under Section 65B(4).²¹

However, the judicial history of the provision indicates that there has been a great deal of inconsistency in terms of how the doctrine evolved in this regard. In the case of *State v. Mohd. Afzal*, the Delhi High Court held that compliance with Section 65B(1) and Section 65B(2) would be sufficient to make the electronic record admissible without having the Section 65B(4) certificate²². Further, the Supreme Court in *State (NCT of*

¹⁷ Vakul Sharma & Seema Sharma, *Information Technology Law and Practice: Cyber Laws and Laws Relating to E-Commerce, Privacy, Social Media, Defamation* (9th edn, LexisNexis 2025) ch. 14.

¹⁸ Indian Evidence Act, 1872, ss. 65A–65B, read with ss. 62–63 (the general primary/secondary evidence provisions).

¹⁹ Information Technology Act, 2000, s. 92 and Second Schedule, inserting ss. 65A–65B into the Indian Evidence Act, 1872, w.e.f. 17 October 2000.

²⁰ Indian Evidence Act, 1872, s. 65A.

²¹ Indian Evidence Act, 1872, s. 65B(2), (4).

²² *State v. Mohd. Afzal*, 2003 (71) DRJ 178 (Del HC).

Delhi) v. Navjot Sandhu held that electronic record could be admitted as secondary evidence under Section 63 and Section 65 in the absence of the Section 65B(4) certificate.²³

However, the law in this regard was overruled in Anvar P.V. v. P.K. Basheer, wherein the Supreme Court declared that Sections 65A and 65B form a self-contained Code dealing with electronic evidence and the fulfillment of Section 65B(4) certificate was imperative, thus expressly rejecting the earlier view expressed in Navjot Sandhu case²⁴. According to the court, the general laws of secondary evidence cannot be applied once a specific procedure has been laid down for that specific evidence²⁵. Such interpretation of the law received significant academic criticism, with Vaidialingam pointing out that the Supreme Court has read an exclusivity into the Section 65B(4) which it does not need.²⁶

VII. STATUTORY STRUCTURE OF ELECTRONIC EVIDENCE UNDER THE BSA: SECTIONS 61–63

These provisions make changes to the way electronic evidence is treated in three successive sections. Section 61 makes it clear that no information which is stored, processed, or transmitted in an electronic form will be refused merely because it is electronic in nature. It deviates from the concept of secondary evidence under the Evidence Act of 1872 and makes electronic records fall within the ambit of primary evidence when it is presented in proper custody²⁷. The Parliamentary Standing Committee on Home Affairs, when analyzing the relevant section of the Bill, approved this change owing to its increasing significance in modern-day trials but pointed out the lack of chain of custody protection²⁸.

²³ State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.

²⁴ Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, paras 22–24.

²⁵ Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, para 17.

²⁶ Ashwini Vaidialingam, 'Authenticating Electronic Evidence: Section 65B, Indian Evidence Act, 1872' (2015) 8 NUJS Law Review 43, 58–61

²⁷ Bharatiya Sakshya Adhiniyam, 2023, s. 61.

²⁸ Parliamentary Standing Committee on Home Affairs, Rajya Sabha, 248th Report on the Bharatiya Sakshya Bill, 2023 (10 November 2023).

Section 62 states that the contents of any electronic record may be proved in terms of Section 63²⁹, having the same role that Section 65A did in the former Act, although not referring to secondary evidence defined as such.

Section 63 states the admissibility conditions. The first three subsections reproduce the old admissibility conditions of Section 65B(2), namely: the computer or the communications device was used routinely for the relevant purpose, relevant information was input into the computer or the communications device routinely, and that the device was working properly at the relevant time³⁰. There are two hallmarks of such a departure from the predecessor legislation. Firstly, Section 63 explicitly applies to 'communication devices' in addition to computers, an extension designed specifically for addressing smartphones and similar technology that the drafters of the 1872 Act could never have considered³¹. Secondly, Section 63(4) provides for the requirement that the certificate regarding the electronic record be provided in the form as prescribed in the Schedule to the Act and split into Part A and Part B, both to be filled in by the relevant individuals – Part A by the individual in charge of the relevant device and Part B by an expert.³² It is the dual certification requirement that differs fundamentally from Section 65B(4) requiring only one certificate from a person in a 'responsible official position'.

In sum, the above restructuring does two quite separate things which this paper considers separately – it classifies electronic records as primary evidence in accordance with Section 61, and raises the bar for certification under Section 63(4). Thus, the common description of the BSA as having 'simplified' or 'relaxed' the certification process can only be correct insofar as the widened scope of applicable technology is concerned.

²⁹ Bharatiya Sakshya Adhiniyam, 2023, s. 62.

³⁰ Bharatiya Sakshya Adhiniyam, 2023, s. 63(2)(3).

³¹ Bharatiya Sakshya Adhiniyam, 2023, s. 63(1)(2).

³² Bharatiya Sakshya Adhiniyam, 2023, s. 63(4) and the Schedule (certificate, Parts A and B).

VIII. COMPARATIVE ANALYSIS: BSA AND IEA ON KEY PARAMETERS

Sections 61 to 63 of the BSA and Sections 65A–65B of the IEA share the common objective of authenticating electronic records, but differ across several specific parameters, summarised below.

Parameter	IEA, 1872 (ss. 65A–65B)	BSA, 2023 (ss. 61–63)
Classification of electronic record	Secondary evidence, proved through a special procedure	Primary evidence under s. 61, where from proper custody
Certificate signatories	Single signature: person in a responsible official position	Dual signature: person in control of device and an expert
Technology covered	Computers and computer output	Computers, communication devices, cloud, IoT, semiconductor memory
Certificate format	No prescribed statutory form	Prescribed Schedule (Parts A and B)
Judicial flexibility to relax requirement	Permitted temporarily (Shafhi Mohammad), then withdrawn (Arjun Panditrao)	Untested; no reported Supreme Court ruling as yet
Chain of custody	No statutory provision	No statutory provision, despite Standing Committee recommendation

IX. THE CERTIFICATION REGIME: SECTION 65B(4) IEA VERSUS SECTION 63(4) BSA

Certificate is the key factor in the admissibility process of electronic evidence in India, and here is where the divergence of the BSA from its predecessor becomes really significant – even counterintuitive.

According to Section 65B(4)³³, one certificate of an individual occupying an official position with respect to the working of the device would be enough to establish the authenticity of electronic document. In this situation, the main problem would be associated with the involvement of third parties (telecommunication service providers, cloud computing services providers, etc.), controlling the relevant device, but having nothing to do with the case.

Clause 63(4) of the BSA³⁴ maintains the certificate requirement but now mandates its submission in the dual-form provided for in Schedule to the Act – one part to be signed by the individual in charge of the device and the other by the expert³⁵. This double-signature arrangement does not solve the initial problem of third-party assistance since it introduces an additional one, that of the lack of statutory definition of who qualifies as an ‘expert’ under the provisions of this Act, thus placing the issue of expert qualifications and availability squarely into the practical sphere³⁶. In smaller cities, which have relatively undeveloped forensic infrastructure, this might be an important restriction.

This concrete example of implementation difficulties shows why. Prosecution witnesses who have already tendered their certificates under the old format of Section 65B were made to re-tender their certificates under the format prescribed in the BSA schedule, many of which did not meet the required format³⁷. It is natural for there to be some friction in the early stages of any procedural system; however, it becomes obvious that the certificate system provided for under the BSA is more burdensome than the previous system.

The conclusion that is being made here, therefore, is limited to the observation that the BSA is not a liberalising document with regards to the law on electronic evidence. As far as certification is concerned, the standard required under the BSA is actually stricter than that of Section 65B(4). Any liberalising feature that the BSA brings with

³³ Indian Evidence Act, 1872, s. 65B(4).

³⁴ Bharatiya Sakshya Adhiniyam, 2023, s. 63(4).

³⁵ Bharatiya Sakshya Adhiniyam, 2023, Schedule, Part B.

³⁶ K&K Litigation, ‘Section 63 BSA 2023: Admissibility of Electronic Evidence’, ksandk.com (4 January 2025) <<https://ksandk.com/litigation/section-63-bharatiya-sakshya-adhiniyam-2023/>>

³⁷ Bar and Bench, ‘Navigating the Transition: Implications of the Bhartiya Sakshya Adhiniyam on Digital Evidence in Ongoing Trials’, Bar and Bench (14 September 2024) <<https://www.barandbench.com/columns/navigating-the-transition-implications-of-the-bhartiya-sakshya-adhiniyam-on-digital-evidence-in-ongoing-trials>>

respect to electronic evidence law can be attributed to the change in classification under Section 61 and the broadening of Section 63.

X. COMPARATIVE INTERNATIONAL PERSPECTIVES ON AUTHENTICATION

A comparative analysis throws into stark light India's continued dependence on certification. Pursuant to the Rules of Evidence under the federal law in the United States, Rules 902(13) and 902(14), enacted in 2017, the authentication of electronically stored information through a certificate ascribing the appropriate hash value or output generated by a computer system is possible without the requirement of foundation testimony of a witness in court³⁸.

In England, the Section 69 of the Police and Criminal Evidence Act of 1984 had previously adopted a presumption-based method for evidence generated by computers in criminal cases; however, this section was subsequently repealed in 1999 due to the opinion that computers have become too commonplace such that proof of correct working in each instance was disproportionate.; From there onwards, the responsibility for raising doubts concerning the reliability of the records has been placed on the party opposing the documents, and not on the party supporting them to get their reliability certified beforehand³⁹. The Civil Evidence Act, 1968 had adopted a largely similar certification process for civil cases, but as pointed out by Chadha and Sivaraman, English courts have always been more forgiving about any procedural deficiencies in the certificates when the reliability of the records has never really been in question⁴⁰.

In light of such comparators, the provision of a second signature provided by experts in Section 63(4) of the BSA is taking India's certification framework towards the contrary direction of the international trend that leans towards reliance on self-certification and presumption for establishing reliability. Such deviation represents a conscious jurisprudential decision, in accordance with the specific concern that has been raised many times before the Standing Committee with respect to the possibility

³⁸ Federal Rules of Evidence (US), r. 902(13)–(14) (as amended 2017); see also r. 901.

³⁹ Police and Criminal Evidence Act, 1984 (UK), s. 69 (repealed by the Youth Justice and Criminal Evidence Act, 1999, s. 60, Sch. 6); Civil Evidence Act, 1968 (UK), s. 5.

⁴⁰ Vaibhav Chadha & Janani Sivaraman, 'Critical Analysis of the Law on Admissibility of Electronic Evidence in India' (2024) Jindal Global Law Review.

of tampering with electronic documents in the Indian forensic and investigative framework⁴¹. Whether such formalism is warranted by the institutional setting in India, or it poses the risk of repeating the mistake made in *Anvar P.V.*, is something that will be addressed at the conclusion of this paper.

XI. CHALLENGES IN ADMISSIBILITY: INSTITUTIONAL AND PRACTICAL ISSUES

Apart from the legislative framework for the certification process, the use of electronic evidence under either of the systems faces limitations due to certain institutional issues that are beyond the capacity of the legislation to solve.

First, there is a lack of definition of the term ‘expert’ in the context of Section 63(4) Schedule, Part B, which means that the accreditation and competency standards will have to be created through practice directions or departmental rules or judicial interpretation of law, an issue which did not arise with the single signature requirement under Section 65B(4)⁴². Second, the forensics infrastructure available to provide the necessary expert certification is available only in urban areas and therefore delays in litigation and investigations in small towns and rural areas is likely to result. Third, although there was a clear recommendation made by the Standing Committee that the chain of custody for electronic and digital evidences collected during investigation should be ensured, there is no mention of this issue in the BSA Act itself.⁴³

Fourth, since the electronic evidence provisions of the BSA became applicable on 1 July 2024⁴⁴, there has not been much judicial opportunity for testing the dual-certification requirement, or how cloud-computing or third-party records should be treated, or if there exists an analogue of the *Shafhi Mohammad* exception. This interpretative ambiguity itself is one transitional cost of legislative change, separate from the institutional costs referred to above.

⁴¹ Parliamentary Standing Committee on Home Affairs, Rajya Sabha, 248th Report on the Bharatiya Sakshya Bill, 2023 (10 November 2023), observations on Clause 57.

⁴² Bharatiya Sakshya Adhiniyam, 2023, s. 63(4); cf. Indian Evidence Act, 1872, s. 65B(4).

⁴³ Parliamentary Standing Committee on Home Affairs, Rajya Sabha, 248th Report on the Bharatiya Sakshya Bill, 2023 (10 November 2023), recommending a statutory chain-of-custody safeguard for electronic and digital records.

⁴⁴ Bharatiya Sakshya Adhiniyam, 2023, s. 1(2).

XII. CONSTITUTIONAL AND PROCEDURAL SAFEGUARDS

The admissibility of electronic evidence needs to be looked at in light of constitutional protections for a fair trial and due process in Article 21 of the Constitution⁴⁵ that are equally applicable in cases of laws like the IEA and the BSA. The requirement of certification under Section 65B(4)⁴⁶ and Section 63(4)⁴⁷ also has a constitutional component to it in that it prevents the conviction of the accused based on electronic evidence that may have been tampered with or is unreliable.

In addition, the right to cross-examine electronic evidence produced in court needs to be considered. Both sides should have a fair chance of examining the genuineness of the electronic records and even the process through which these records were obtained especially when the collection of such records involves the forensic expert or any intermediary. The extension of the definition of certification to an independent expert under the BSA, in theory, makes this protection better because it adds an extra, supposedly neutral, layer of accountability but only if the certificate issued by the expert is indeed independent and not simply an afterthought to investigative certificates.

Issues of privacy must also be considered in connection with the use of electronic evidence due to the growing recognition of the duties to preserve privacy in light of the Digital Personal Data Protection Act, 2023⁴⁸. The issue of the use of electronic evidence and its possible conflicts with the aforementioned privacy issues must be resolved and, to some extent, goes well outside of the scope of this paper. Taken together, the Article 21's guarantee of fair trial and the right to cross-examination along with the emerging privacy rights create a multi-level check on the procedural framework established by both Acts, in addition to the certification procedure analyzed above.

XIII. CONCLUSION

However, a major takeaway from this paper contradicts the prevalent belief concerning the Bharatiya Sakshya Adhiniyam, 2023: this act is seen as relaxing

⁴⁵ Constitution of India, art. 21.

⁴⁶ Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

⁴⁷ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

⁴⁸ Digital Personal Data Protection Act, 2023, s. 4.

procedural formalism regarding the use of electronic evidence as prescribed by the Indian Evidence Act. However, on careful textual analysis, the former holds true only to some extent. In relation to two areas, the BSA actually makes it easier; first, it changes the classification of electronic records from secondary to primary evidence in Section 61, and second, it expands the scope of technology referred to in Section 63 to cover communication devices, cloud computing, IoT, and semiconductor memory. Yet, when it comes to certification specifically, the requirement of two signatures in Section 63(4) is in fact more stringent compared to the earlier requirement of a single signature certificate under Section 65B(4).

The second finding is about the process of adjudication. The doctrinal history that was discussed above in connection with Mohd. Afzal, Navjot Sandhu, Anvar P.V., Shafhi Mohammad and Arjun Panditrao Khotkar indicates that twenty years and six key decisions were necessary to consolidate the interpretation of the regime introduced by the IEA in a fixed and rigid form. The BSA is in this very interpretive space without having any established precedents because Section 63 has never been considered by the Supreme Court. In any event, whatever flexibility of interpretation of Section 63(4) courts allow will certainly reflect the debates around Section 65B(4).

The third observation made through the international comparative analysis is that the certification-based system in India has now become increasingly divergent from international systems as compared to its position prior to the enactment of the BSA. The shift towards self-authentication in the United States in light of Federal Rules of Evidence 902(13)-(14) and the move away from reliance on certificates to create presumption of reliability in the United Kingdom since the repeal of Section 69 of the Police and Criminal Evidence Act, 1984 indicate that the reliability challenge lies with the opposite party.

Unresolved Issues

- a. Qualifications of an 'expert' in relation to Part B of the Schedule to Section 63 are not defined in statute, but rather developed in practice;
- b. Parliamentary Standing Committee's suggestion of incorporating a statutory chain-of-custody obligation for electronic and digital records is yet to be included into the BSA, and its future in subordinate rules to the Bharatiya Nagarik Suraksha Sanhita, 2023 is uncertain;

- c. there has been no interpretation of Section 63(4) in the form of a Supreme Court judgment, hence the question of whether a similar relaxation of the Shafhi Mohammad principle would apply if obtaining dual certifications is truly impossible;
- d. There remains the transitional issue of what to do with electronic records that originated, or have been certified, under the IEA, but continue to be used in ongoing trials after 1 July 2024 – one of which there is no clear answer in the text of the BSA; and
- e. Access to qualified forensic experts in non-metropolitan India remains an empirical issue unresolved by this paper, but which speaks directly to whether Section 63(4) operates as intended.

Recommendations

- a. That subordinate rules or practice directions regarding the qualification, accreditation, and empanelment criteria for the term ‘experts’ as per Part B of the Section 63 Schedule may be issued by the Ministry of Home Affairs or any other rule-making authority, to ensure that the said provision is not made into a de facto impediment to the production of electronic evidence;
- b. That the chain-of-custody protection suggested by the Standing Committee may be provided, whenever possible, either through an amendment to the BSA or through binding rules under the Bharatiya Nagarik Suraksha Sanhita, 2023, and not left merely to administrative practice;
- c. That judicial academies must give priority to training programs on the practical working of Section 63(4) along with its Schedule for trial court judges in light of the large number of cases involving electronic evidence; and
- d. That the courts must, in case Section 63(4) ever comes to be tested in litigation, be mindful of the possibility of creating the same hard-line exclusionary principle as existed under Anvar P.V., and evaluate whether the more flexible and fact-based principle, as was briefly applicable in Shafhi Mohammad, ought to apply where dual certification cannot realistically be obtained; and