2026 Volume: 02 Issue: 04 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-09

"ADMISSIBILITY OF ELECTRONIC EVIDENCE UNDER BHARATIYA SAKSHYA ADHINIYAM, 2023: A CRITICAL ANALYSIS"

[*1]Manasi Pandey, [2]Dr. Shaiwalini Singh

[1]L.L.M (Criminal Law) Student: Amity University, Lucknow.

[2]*Assistant Professor Grade I,* Amity Law School, Amity University Lucknow Campus.

Article Received: 05 March 2026
Article Revised: 23 March 2026
Published on: 13 April 2026

***Corresponding Author: Manasi Pandey**
L.L.M (Criminal Law) Student: Amity University, Lucknow.

DOI: https://doi-doi.org/101555/ijrpa.2869

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which entered into operation on 1 July 2024 upon superseding the Indian Evidence Act, 1872, establishes a materially reconstituted regime for the reception of electronic records in Indian judicial proceedings. This paper undertakes a critical appraisal of the BSA's provisions pertaining to electronic evidence, tracing their doctrinal genealogy through the deeply contested Section 65B mechanism and the watershed pronouncements of the Supreme Court in Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020). The central contention advanced is that whilst the BSA succeeds in resolving numerous interpretive uncertainties that had long beset its predecessor statute, consequential lacunae continue to subsist in relation to the certification requirement, cloud-hosted data, and algorithmically generated records. The paper concludes by formulating recommendations directed to both Parliament and the judiciary to ensure that India's law of electronic evidence is rendered adequate to the demands of the contemporary digital environment.

KEYWORDS: *BSA 2023, Electronic Evidence, Section 63, Section 65B IEA, Anvar P.V., Khotkar, Digital Evidence India, Certificate Requirement.*

I. INTRODUCTION

In an era defined by pervasive technological change, India's criminal justice system has been compelled to fundamentally reconceive its evidentiary architecture to remain consonant with the exigencies of the digital age. The evidentiary substratum of contemporary criminal

litigation — encompassing offences ranging from homicide and financial fraud to sophisticated cybercrime — no longer resides principally in paper records but is distributed across the digital infrastructure of mobile devices, electronic mail repositories, closed-circuit surveillance networks, instant messaging applications, and cloud computing platforms. The legal principles governing the conditions under which such materials may be tendered before a court, and the procedural form in which they must be presented, have consequently assumed a position of cardinal practical importance within Indian evidence law. It is against this jurisprudential backdrop that the promulgation of the Bharatiya Sakshya Adhiniyam, 2023 — which came into force on 1 July 2024, thereby displacing the Indian Evidence Act, 1872 — acquires its profound legislative significance. The BSA constitutes the first thoroughgoing restatement of India's general law of evidence in excess of a century and a half, and its provisions governing electronic records — concentrated primarily within Sections 57 to 63 — represent among its most consequential contributions to the legal order.

The practical stakes attending a coherent and well-calibrated framework for electronic evidence are substantial. In 2022, the National Crime Records Bureau (NCRB) documented in excess of 966,000 cognisable offences under cybercrime-related statutory provisions, with digital evidence constituting a material component of the prosecution case across a wide spectrum of serious criminal matters. Yet throughout much of the period since electronic evidence was first accorded a statutory footing in Indian law through Section 65B of the IEA — introduced by the Information Technology Act, 2000 — courts, investigative agencies, and members of the Bar were confronted with a regime that was technically exacting, frequently misunderstood, and the site of irreconcilable judicial conflict. The BSA's endeavour to supplant and improve upon that framework warrants rigorous critical scrutiny, which this paper sets out to provide.

II. The Section 65B Regime Under the Indian Evidence Act, 1872: Background and Problems

An adequate appreciation of the BSA's provisions necessitates a prior understanding of the framework they were designed to replace. Sections 65A and 65B were grafted onto the Indian Evidence Act, 1872 by the Information Technology Act, 2000, with the object of establishing a statutory basis for the reception of computer-generated documents as secondary evidence. Section 65B stipulated that any printed reproduction or electronic copy of a computer-generated record was required to be accompanied by a certificate, executed by a person

occupying a responsible official position, attesting to four distinct conditions: that the computer in question had been habitually employed in the relevant activities; that it had been functioning in proper working order during the material period; that the information had been supplied to it in the ordinary course of operations; and that the document accurately reproduced the stored data. The certificate requirement enshrined in Section 65B(4) proved to be the most contentious provision in this framework, for the straightforward reason that the legislature had not plainly specified the legal consequences of a failure to obtain the requisite certification.

The first authoritative Supreme Court pronouncement on this question arose in State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600 — the Parliament Attack Case — wherein the court adopted the position that electronic records were susceptible of proof through oral testimony, without strict adherence to the Section 65B mechanism, wherever the circumstances rendered such an approach appropriate. This interpretive approach was, however, definitively repudiated by a three-judge bench of the Supreme Court in *Anvar P.V. v. P.K. Basheer and Others (2014) 10 SCC 473,* which held that the Section 65B certificate constituted a mandatory precondition for the admissibility of electronic records as secondary evidence, admitting of no substitution by viva voce evidence. The court declared that Sections 65A and 65B together formed 'a complete code' for the proof of electronic records, and that non-compliance with the certification requirement necessarily rendered the evidence inadmissible as a matter of law. This ruling, though it furnished much-needed doctrinal coherence, precipitated immediate practical dislocation: a considerable body of pending criminal prosecutions had already placed electronic evidence before courts in the absence of a Section 65B certificate, and in the wake of Anvar P.V., the evidentiary value of that material was fundamentally imperilled.

The matter received its definitive resolution from a five-judge constitutional bench of the Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1, which affirmed the obligatory character of the certification requirement but made two pivotal supplementary holdings. First, the court ruled that a trial court possesses the power — and is indeed under a duty — to direct any person in custody of a Section 65B certificate to produce it, upon the application of the party seeking to admit the electronic record in evidence. Second, and of direct relevance to the present analysis, the court articulated a clear demarcation between primary and secondary forms of electronic evidence: where the original device itself is produced before the court and its contents are demonstrated directly

therefrom, such evidence constitutes primary evidence within the meaning of Section 62 of the IEA, to which no certification requirement attaches. The certificate obligation operates exclusively in relation to copies, printouts, and reproductions — that is, secondary electronic evidence. This primary-secondary dichotomy, whilst jurisprudentially defensible, left unresolved a fundamental question that the IEA framework was structurally ill-equipped to answer: where, precisely, does the 'original' reside when data is housed in cloud infrastructure?

III. The BSA 2023: A New Framework for Electronic Evidence

The Bharatiya Sakshya Adhiniyam, 2023 is directly constructed upon the judicial foundations established by Anvar P.V. and Khotkar, incorporating their respective holdings into positive statutory form whilst endeavouring to address the limitations those decisions exposed. The definition of 'electronic record' in Section 2(1)(e) of the BSA is deliberately drafted in expansive, technology-neutral terms, encompassing any data, record, image, or sound stored, transmitted, or received in electronic form or on microfilm or computer-generated microfiche. This represents a material advance over the narrower 'computer output' formulation employed in Section 65B, which had furnished the basis for contentions in certain courts that devices other than conventional computers — including smartphones, GPS receivers, embedded electronic systems, and devices within the Internet of Things ecosystem — fell outside the ambit of the statutory admissibility framework because they did not generate 'computer output' in the technical sense contemplated by the provision.

The admissibility of electronic records as secondary evidence is governed by Section 63 of the BSA, which constitutes the direct statutory successor to Section 65B of the IEA. Section 63 retains the certificate requirement in a reconstituted and clarified form. The certificate must be furnished by a person who occupies a responsible official position in relation to the management of the relevant device or system from which the electronic record originated, and must particularise the identity of the device, the modalities of production of the record, and the circumstances bearing on its integrity. A provision of particular significance is that Section 63 of the BSA expressly confers upon courts the power to direct the production of the certificate in cases where it has not been voluntarily furnished — thereby elevating the Khotkar direction to the status of a statutory mandate and eliminating the doctrinal uncertainty that attended the existence of this power under the former IEA regime. The BSA also introduces a degree of procedural adaptability that was conspicuously absent from the

antecedent Section 65B: where the certificate has not been procured at the juncture at which the electronic record is first tendered, the court is empowered to allow the tendering party a reasonable period within which to produce it, rather than treating its initial non-production as an absolute and immediate bar to admissibility. This modification is a direct legislative response to the disproportionate consequences that the rigorous Anvar P.V. approach generated in numerous cases, where prosecutions were effectively defeated not by reason of any intrinsic unreliability in the evidence but solely because the certification had not been obtained within the requisite time.

IV. Critical Analysis: What the BSA Gets Right and Where Gaps Remain

The electronic evidence framework established by the BSA merits recognition for a number of genuine and substantive improvements over its predecessor. The technology-neutral scope of the definition of 'electronic record' ensures that the admissibility regime will operate across the full spectrum of digital evidence modalities in contemporary use and those likely to emerge in the foreseeable future. The legislative codification of the court's power to compel the production of the certificate removes a significant practical impediment that subsisted under Khotkar's judge-made direction. And the introduction of procedural flexibility in the timing of compliance reflects a mature adjudicative policy that subordinates rigid technical formalism to the reliable ascertainment of factual truth. These are genuine and substantial advances that will be of tangible utility to lawyers and judges engaged in forensic practice on a daily basis.

Nevertheless, the BSA's framework also leaves significant and consequential lacunae unaddressed. The most substantial deficiency concerns the admissibility of electronic records maintained on cloud platforms operated by foreign technology enterprises — a category of evidence that now constitutes the evidentiary foundation of a very considerable proportion of cybercrime prosecutions in India. Where an investigating authority requires call detail records from a domestic telecommunications operator, the process of obtaining a Section 63 certificate from the operator's designated official is relatively straightforward. However, where the evidence sought is held on the servers of an American social media corporation, an international electronic mail service provider, or a global cloud storage enterprise, the identification of a party who can legitimately furnish a Section 63 BSA certificate becomes profoundly problematic. Such companies are subject to the domestic laws of their home jurisdictions — predominantly the legal regimes of the United States and the European Union

— and are frequently either unwilling or legally precluded from issuing certifications in conformity with Indian domestic evidentiary law. The BSA has not established any specific mechanism for addressing this practical impasse, leaving investigators, prosecutors, and courts to navigate its complexities without clear statutory guidance.

A second significant lacuna is the BSA's complete absence of any provision governing AI-generated records. As artificial intelligence systems are deployed with increasing frequency in criminal investigation — for purposes including facial recognition, automated analysis of financial transactions, predictive policing outputs, and digital forensic examination — courts will be presented with increasing regularity with records produced not by a human operator but by an automated algorithmic process. The certificate requirement under Section 63 presupposes the existence of a human certifier capable of attesting to the proper functioning of the relevant system; however, an AI-generated record may not possess any single identifiable human author or custodian who can meaningfully certify the reliability of the specific output in question. The development of a jurisprudence adequate to this challenge will necessitate either targeted legislative amendment or a creative judicial construction of the existing BSA provisions.

V. Constitutional Dimension: Right to Fair Trial and Electronic Evidence

Any rigorous critical analysis of India's law of electronic evidence must engage with its constitutional dimension. The right to a fair trial is established as a fundamental right under Article 21 of the Constitution of India, as affirmed consistently by the Supreme Court in cases including Maneka Gandhi v. Union of India (1978) 1 SCC 248 and Hussainara Khatoon v. State of Bihar (1979) 3 SCC 532. This constitutional guarantee has direct and far-reaching implications for the law of electronic evidence, because an accused person who is convicted on the basis of electronic evidence that they have been unable to contest meaningfully — on account of the opacity of the methodology of its generation, the absence of a verified chain of custody, or the inaccessibility of a proprietary algorithm that produced it — has not received the fair trial to which they are entitled under the Constitution. The Supreme Court's recognition of the right to privacy as a fundamental right under Article 21 in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 also carries significant consequences for the manner in which electronic evidence is collected and preserved: evidence acquired through unlawful surveillance or in derogation of the proportionality standard enunciated in

Puttaswamy may be susceptible to challenge on constitutional grounds notwithstanding its technical compliance with the admissibility requirements of Section 63 BSA.

VI. RECOMMENDATIONS

On the basis of the analysis set out in the preceding sections, this paper advances three principal recommendations. First, Parliament ought to amend the BSA so as to enact a specific provision addressing the admissibility of electronic records obtained from foreign-based service providers, establishing either a mutual recognition mechanism for foreign evidentiary certifications or a bespoke procedure for obtaining court-directed authentication of such records. This is a legislative priority that admits of no deferral, given the centrality of cloud-hosted digital evidence to the prosecution of cybercrime in India. Second, the Supreme Court or the Law Commission ought to develop authoritative guidelines governing the authentication and admissibility of AI-generated records in criminal proceedings, specifying the technical standards such records must satisfy, the qualifications required of expert witnesses called to attest to their reliability, and the procedural entitlements of accused persons to challenge the underlying algorithmic architecture. Third, the Bar Council of India and the National Judicial Academy should make training in digital evidence law mandatory for all practising advocates and judicial officers, thereby ensuring that the enhanced statutory framework of the BSA is translated into competent and consistent forensic practice throughout the country.

VII. CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023 marks a significant jurisprudential advance in India's law of electronic evidence. Through its expansion of the definition of electronic record, its statutory entrenchment of the Khotkar directions on certificate production, and its introduction of procedural flexibility in the timing of compliance, the BSA fashions a more practicable and more equitable framework than the regime it has supplanted. The protracted doctrinal journey — from the analytical uncertainty of Navjot Sandhu, through the clarifying precision of Anvar P.V., and thence to the constitutional bench settlement in Khotkar — has, at length, attained a statutory expression that reflects the highest achievements of India's judicial engagement with electronic evidence. Yet the task remains incomplete. The challenges posed by cloud-stored evidence, algorithmically generated records, and cross-border data governance constitute the next frontier of electronic evidence law — a frontier that the BSA has acknowledged but not yet traversed. The lesson drawn from a sustained

engagement with this field of law is that legal doctrine is never fully consummated; in a living constitutional democracy, it remains perpetually subject to revision and renewal. The imperative now is to ensure that the legislative, judicial, and institutional actors entrusted with the development of India's evidence law approach that responsibility with the urgency, the technical fluency, and the constitutional fidelity that the digital age demands of them.

REFERENCES

Cases

1. Anvar P.V. v. P.K. Basheer and Others, (2014) 10 SCC 473 — Supreme Court of India
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 — Supreme Court of India (5-judge constitutional bench)
3. Hussainara Khatoon v. Home Secretary, State of Bihar, (1979) 3 SCC 532 — Supreme Court of India
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 — Supreme Court of India
5. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 — Supreme Court of India
6. Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 — Supreme Court of India
7. Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570 — Supreme Court of India
8. State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, (2005) 11 SCC 600 — Supreme Court of India

Legislation

9. Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023) — Ministry of Law and Justice, Government of India. In force 1 July 2024
10. Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023) — Government of India
11. Constitution of India, 1950 — Articles 14, 20, 21 — Government of India
12. Indian Evidence Act, 1872 (Act No. 1 of 1872) — Government of British India [repealed 1 July 2024]
13. Information Technology Act, 2000 (Act No. 21 of 2000, as amended 2008) — Government of India

Books and Articles

14. Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press, Waltham

15. Mason, S. (ed.) (2017). Electronic Evidence (4th ed.). Institute of Advanced Legal Studies, London
16. National Crime Records Bureau (2022). Crime in India Report 2022. MHA, Government of India
17. Pattanayak, S. (2021). Electronic Evidence in Indian Courts. Eastern Book Company, Lucknow
18. Sharma, A. and Gupta, R. (2020). Digital Forensics and Cyber Law in India. Eastern Book Company, Lucknow
19. Singh, A.K. (2022). Electronic Evidence Under Indian Law: Post-Khotkar Framework. Indian Law Review, 6(1), pp. 45–78
20. Srivastava, S. (2023). The Bharatiya Sakshya Adhiniyam 2023: A Comparative Analysis. Journal of Indian Law and Society, 14(2), pp. 112–145