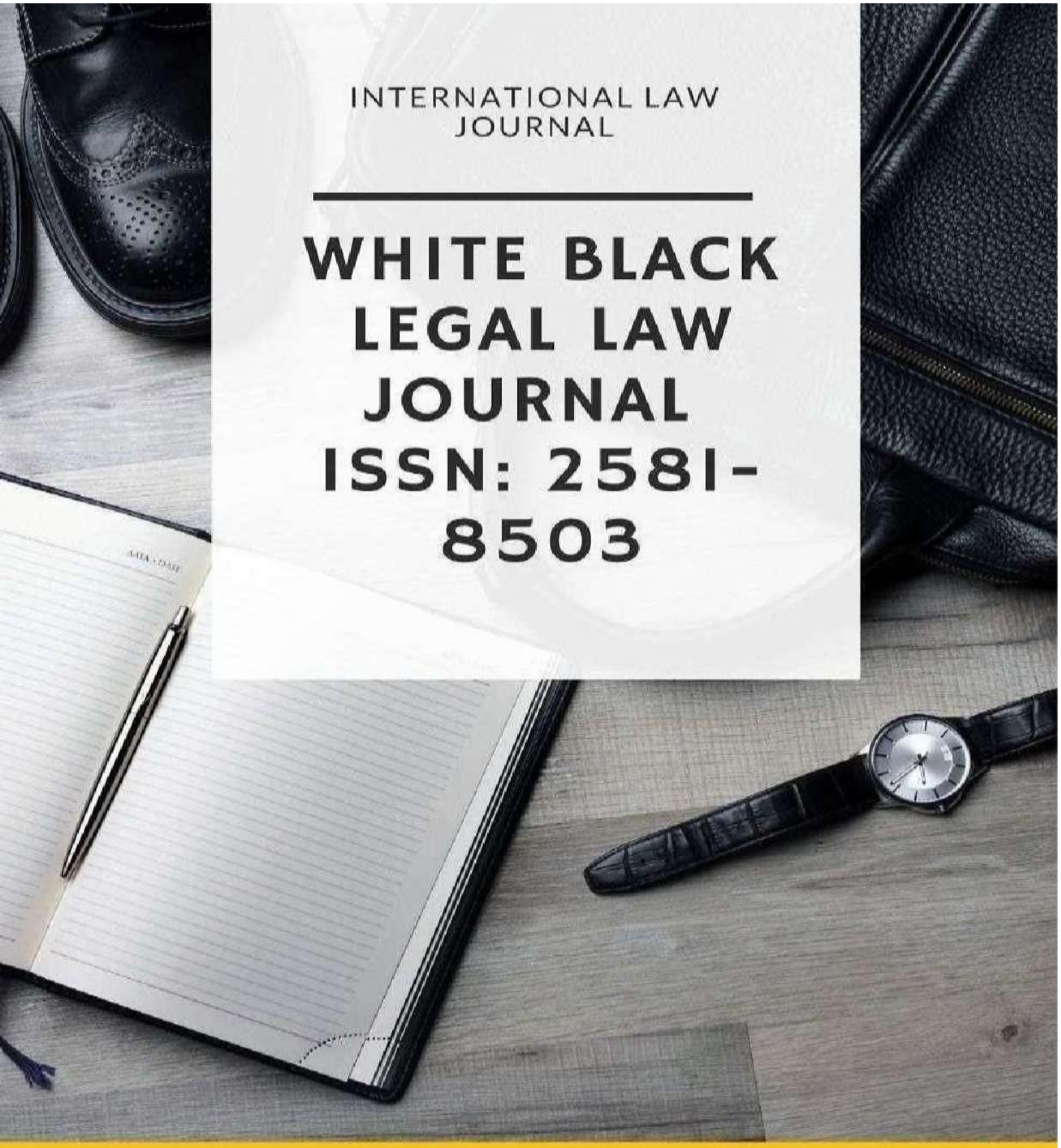

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

ADMISSIBILITY AND EVIDENTIARY VALUE OF ELECTRONIC RECORDS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023: CRITICAL ISSUES AT THE INTERSECTION OF LAW, TECHNOLOGY, AND JUSTICE

AUTHORED BY - ANKIT KUMAR
Ph.D (Law) Scholar
Baba Mastnath University Rohtak

CO –AUTHOR - DR.SEEMA DEVI
Associate professor Faculty of Law, BMU, Rohtak

ABSTRACT

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) to replace the Indian Evidence Act, 1872 represents India's most significant statutory reform of the law of evidence in over a century and a half. Among the most consequential aspects of this legislative overhaul is the new framework governing the admissibility, authentication, and evidentiary weight of electronic records. This paper undertakes a comprehensive critical analysis of the BSA's provisions on electronic evidence, examining Sections 61-65 and related provisions against the constitutional guarantees of Articles 20 and 21, the emerging global jurisprudence on digital evidence, and the practical imperatives of criminal adjudication in the digital age. The paper traces the evolution of India's electronic evidence law from the foundational Section 65B of the Indian Evidence Act as interpreted by the Supreme Court in Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal through to the new statutory framework. It critically evaluates the BSA's treatment of the certificate requirement for electronic records, the admissibility of electronic communications, the challenges of authenticating artificial intelligence-generated evidence, and the implications of the new provisions for the rights of the accused, particularly the privilege against self-incrimination. The paper further engages with comparative approaches in the United States, the United Kingdom, and Singapore. The study concludes that while the BSA makes welcome improvements, it leaves unresolved several critical questions of authentication, reliability, and privilege that will inevitably generate significant litigation.

Keywords: *Bharatiya Sakshya Adhiniyam 2023; Electronic Evidence; Digital Records; Section 65B; Certificate Requirement; Authentication; Artificial Intelligence Evidence; Right Against Self-Incrimination; Criminal Justice; Evidence Law India*

INTRODUCTION

The Indian Evidence Act of 1872, drafted by Sir James Fitzjames Stephen, governed the admissibility of evidence in Indian courts for over 150 years. Designed for an age of paper documents, oral testimony, and physical objects, the Act was progressively amended to accommodate technological change most significantly through the Information Technology Act, 2000, which inserted Sections 65A and 65B to create a framework for the admissibility of electronic records.[1]

The Bharatiya Sakshya Adhiniyam, 2023, which came into force on July 1, 2024, replaces the Indian Evidence Act in its entirety. The BSA represents a comprehensive restatement of the law of evidence, restructured and updated to reflect contemporary evidentiary challenges. The provisions governing electronic evidence occupy a central position in this reform, given that an overwhelming proportion of communications, transactions, and records in modern India and therefore an overwhelming proportion of evidence in criminal proceedings exist in electronic form.[2]

The significance of the electronic evidence framework extends beyond mere procedural technicality. In criminal cases, the question of whether a WhatsApp message, an email trail, a CCTV recording, a mobile call data record, or a metadata-laden digital file is admissible and if so, what weight it ought to receive can determine guilt or innocence, liberty or incarceration. The stakes are therefore both procedurally and constitutionally profound.

The Supreme Court's evolving jurisprudence on Section 65B of the Indian Evidence Act had by 2020 settled into a complex set of rules regarding the certificate requirement for electronic records, distinguishing between primary and secondary evidence of electronic records, and addressing the question of who may furnish the certificate.[3]

[1] Section 65B, Indian Evidence Act, 1872 (as inserted by Section 92, Information Technology Act, 2000). See Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing, 6th edn, 2020), Chapter 9.
[2] Statement of Objects and Reasons, Bharatiya Sakshya Adhiniyam Bill, 2023, introduced in Lok Sabha on August 11, 2023.
[3] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, per Nariman J. (Constitution Bench), consolidating the Section 65B jurisprudence.

The BSA now operates in this contested jurisprudential landscape. This paper examines whether the BSA's electronic evidence provisions resolve existing problems, introduce new complexities, and adequately address the constitutional dimensions of digital evidence in criminal proceedings. The paper is structured to provide a thorough contextual, doctrinal, comparative, and normative analysis.

LITERATURE REVIEW

Evolution of Electronic Evidence Law in India

The legislative history of electronic evidence in India begins with the Information Technology Act, 2000, which through its amendments to the Indian Evidence Act inserted the framework for the admissibility of electronic records under Sections 65A and 65B. The conditions specified in Section 65B particularly the requirement for a certificate from a person responsible for the operation of the computer proved to be a source of sustained judicial controversy.[4]

In State (NCT of Delhi) v. Navjot Sandhu (the Parliament Attack Case), the Supreme Court held that secondary evidence of electronic records could be led under Sections 63 and 65 of the Indian Evidence Act without the certificate under Section 65B.[5] This position was directly overruled by a three-judge bench in Anvar P.V. v. P.K. Basheer, which held that Section 65B is a complete code for the admission of electronic records and that the certificate is mandatory where secondary evidence of an electronic record is sought to be adduced.[6]

The Supreme Court further refined the law in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, where a Constitution Bench held that the certificate under Section 65B(4) is a condition precedent for the admissibility of electronic records as secondary evidence, but that a party who is not in a position to obtain the certificate may seek production through court process.[7]

Scholarship on Digital Evidence and Criminal Justice

International scholarship on digital evidence has grappled with the challenges of authentication, chain of custody, metadata integrity, and the reliability of electronic records produced by automated systems. Kerr's influential work on the Fourth Amendment in cyberspace explores the tension between traditional evidentiary doctrines designed for physical

[4] V.C. Govindan Nair (ed.), Evidence Law in India (Asia Law House, 2003), pp. 234-256.
[5] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[6] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 per Joseph Kurien J.: 'Section 65B(4) is a condition precedent to the admissibility of evidence by way of electronic record.'
[7] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

objects and the unique characteristics of digital data.[8]

Indian scholarship on electronic evidence has been dominated by practitioner commentaries, including the exhaustive work of Justice S.P. Bharucha and commentaries by Nandan Kamath and Pavan Duggal on cyber law and electronic evidence.[9]

The emergence of artificial intelligence-generated content as potential evidence from deepfakes to AI-generated voice recordings to algorithm-determined outputs has generated a growing body of scholarship questioning the adequacy of traditional authentication doctrines.[10]

Critiques of the BSA Electronic Evidence Framework

Early commentaries on the BSA, particularly from the Bangalore-based Internet Freedom Foundation and the Centre for Internet and Society, have flagged concerns about the BSA's treatment of electronic records, including the apparent dilution of the certificate requirement and the absence of provisions addressing AI-generated evidence, blockchain records, and cloud-stored data.

The Parliamentary Standing Committee on Home Affairs in its report noted that the BSA provisions on electronic records require further elaboration, particularly regarding the certification of electronic records in automated transactions and the evidentiary status of algorithmic outputs.[11]

RESEARCH PROBLEM

The admission of electronic evidence in criminal proceedings implicates at least three distinct sets of concerns. The first is the reliability concern: electronic records are uniquely susceptible to alteration, fabrication, and metadata manipulation, raising questions about the probative value that courts should assign to unverified digital material. The second is the rights concern: the compelled production of electronic records whether stored in personal devices, cloud accounts, or encrypted communications may implicate the right against self-incrimination under Article 20(3) and the right to privacy under Article 21. The third is the systemic concern: the growing prosecution dependence on electronic evidence, including AI-generated outputs, risks a crisis of epistemic authority if the legal framework does not keep pace with

[8] Orin S. Kerr, 'Searches and Seizures in a Digital World' (2005) 119 Harvard Law Review 531.
[9] Pavan Duggal, Cyber Law: The Indian Perspective (Saakshar Law Publications, 4th edn, 2022), Chapters 11-14.
[10] Ryan Calo and Danielle Citron, 'The Automated Administrative State' (2021) 106 Minnesota Law Review 2051 (exploring AI-generated outputs as legal evidence). Internet Freedom Foundation, Analysis of the Bharatiya Sakshya Adhiniyam, 2023 (October 2023), pp. 12-18.
[11] Parliamentary Standing Committee on Home Affairs, Report on the Bharatiya Sakshya Adhiniyam, 2023 (November 2023), paras 9-14.

technological developments.

The BSA's electronic evidence framework must be evaluated against all three concerns. The paper's central research problem is: Does the BSA, 2023 establish an adequate, constitutionally sound, and technologically responsive framework for the admissibility and evaluation of electronic records in Indian criminal proceedings?

OBJECTIVES OF THE STUDY

The study pursues the following specific objectives:

(i) To map and compare the electronic evidence provisions of the BSA, 2023 with those of the Indian Evidence Act, 1872 (as amended).

(ii) To critically evaluate the BSA's certificate requirement and authentication framework for electronic records.

(iii) To analyze the constitutional dimensions of the BSA's electronic evidence provisions, particularly concerning the right against self-incrimination and the right to privacy.

(iv) To assess the BSA's capacity to accommodate emerging categories of digital evidence, including AI-generated content, encrypted communications, blockchain records, and cloud-stored data.

(v) To compare the BSA framework with approaches in the United States, United Kingdom, Singapore, and the European Union.

(vi) To formulate specific recommendations for legislative amendment and judicial interpretation to strengthen the BSA's electronic evidence framework.

RESEARCH QUESTIONS / HYPOTHESES

Research Questions

Primary Question: Does the Bharatiya Sakshya Adhiniyam, 2023 provide an adequate and constitutionally sound framework for the admissibility, authentication, and evaluation of electronic evidence in criminal proceedings?

Secondary Questions:

(a) Does the BSA's treatment of the certificate requirement for electronic records resolve the contradictions generated by the Section 65B jurisprudence, or does it introduce new interpretive difficulties?

(b) Does the BSA adequately address the admissibility and weight of AI-generated evidence in criminal proceedings?

(c) To what extent do the BSA provisions on electronic evidence comply with the constitutional right against self-incrimination under Article 20(3)?

(d) How does the BSA framework on electronic evidence compare with the best practices adopted in leading jurisdictions?

(e) What are the implications of the BSA's electronic evidence provisions for the right to a fair trial of the accused?

Hypotheses

H1: The BSA, 2023 does not fully resolve the interpretive controversies generated by the Section 65B framework of the Indian Evidence Act and will generate fresh rounds of litigation on authentication and certification.

H2: The BSA contains significant lacunae regarding AI-generated evidence, blockchain records, and cloud data, which will prove inadequate in the face of rapidly evolving forensic practices.

H3: Certain BSA provisions relating to the compelled production of electronic records may not withstand constitutional scrutiny under Articles 20(3) and 21.

THEORETICAL / CONCEPTUAL FRAMEWORK

The paper is situated within the framework of evidence theory, specifically the epistemic approach developed by William Twining, which evaluates rules of evidence by their contribution to accurate fact-finding and the avoidance of wrongful conviction.[12]

The paper additionally draws on the constitutional theory of informational privacy developed by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India, which established privacy as a fundamental right under Article 21 and identified informational self-determination as a core component of that right.[13]

The doctrinal framework of authentication theory in evidence law as elaborated by Edward Imwinkelried's work on the authentication of electronic records provides the analytical

[12] William Twining, Rethinking Evidence: Exploratory Essays (Cambridge University Press, 2nd edn, 2006), pp. 1-45.
[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 per Chandrachud J. (concurring): 'Informational privacy is a facet of the right to privacy.'

vocabulary for evaluating the BSA's certificate and authentication requirements.[14]

Finally, the paper engages with the growing interdisciplinary literature on algorithmic accountability and the law, which questions the admissibility and weight of outputs generated by opaque AI systems in legal proceedings a concern that Indian courts will increasingly be required to address.

RESEARCH METHODOLOGY

Doctrinal Research

The study involves a comprehensive textual and contextual analysis of the electronic evidence provisions of the BSA, 2023, cross-referenced against the Indian Evidence Act, 1872 (as amended by the IT Act, 2000), relevant constitutional provisions, and the body of Supreme Court and High Court jurisprudence on Section 65B. The analysis is organized thematically around key issues: authentication, the certificate requirement, compelled production, and AI-generated evidence.

Case Law Analysis

A systematic review of Supreme Court and High Court decisions on Section 65B and electronic evidence has been conducted, with particular attention to the trilogy of Navjot Sandhu, Anvar P.V., and Arjun Panditrao as the foundational cases, and to subsequent High Court developments interpreting the certificate requirement in specific evidentiary contexts.

Comparative Law

Comparative analysis draws on: the Federal Rules of Evidence (US), particularly Rules 901 and 902 on authentication; the UK's Criminal Justice Act, 2003 and the Police and Criminal Evidence Act, 1984 on hearsay and electronic records; Singapore's Electronic Transactions Act and Evidence Act on computer output; and the EU's eIDAS Regulation on electronic signatures and authentication.[15]

Interdisciplinary Engagement

The paper engages with technical literature on forensic computing, metadata analysis, blockchain authentication, and the reliability of machine learning outputs as necessary

[14] Edward J. Imwinkelried, Evidentiary Foundations (Carolina Academic Press, 10th edn, 2020), Chapter 14.
[15] Stephen Mason, Electronic Evidence (LexisNexis, 4th edn, 2017), Chapters 4-7.

background for the legal analysis. This is supplemented by recent judicial and regulatory reports from the UK Forensic Science Regulator, the US National Institute of Standards and Technology (NIST), and INTERPOL's Digital Forensics Working Group.

DATA ANALYSIS / FINDINGS

The Certificate Requirement under the BSA

Section 63 of the BSA re-enacts the certificate requirement for electronic records as secondary evidence, but with certain modifications. The BSA introduces a distinction between records produced by automated computer systems in the ordinary course of business (for which a simplified certificate may suffice) and records produced by individual user activity (which require the full certificate). This distinction, while pragmatically sensible, introduces new definitional questions about what constitutes an 'automated' system in the context of AI-assisted or algorithmically curated platforms such as social media.[16]

The BSA also addresses the Arjun Panditrao problem where the party seeking to produce electronic evidence does not have access to the system generating the record and cannot obtain the certificate by providing for court-directed production and certification. However, the mechanism is procedurally complex and may impose significant delays in criminal proceedings.[17]

Electronic Communications as Evidence

A significant proportion of criminal evidence now consists of messaging application data WhatsApp, Telegram, Signal, and other platforms. The BSA does not contain specific provisions addressing the admissibility of messages extracted from such platforms, leaving courts to apply the general electronic records framework. This is particularly problematic where end-to-end encryption renders the service provider unable to produce the content, and where law enforcement agencies extract messages through device seizure rather than platform access.[18]

The chain of custody requirement for device-extracted messages is particularly challenging: the integrity of the extraction process, the use of forensic tools that may or may not be documented or approved, and the risk of contamination during examination all potentially affect the reliability of the resulting evidence. The BSA does not prescribe standards for

[16] Section 63, Bharatiya Sakshya Adhiniyam, 2023.
[17] Section 63(4), Bharatiya Sakshya Adhiniyam, 2023; see also Arjun Panditrao, supra note 7 at para 48.
[18] Eoghan Casey, 'Standards for Digital Evidence' (2011) 8(2) Digital Investigation 1, pp. 3-9.

forensic extraction tools or processes, leaving this to judicial evaluation on a case-by-case basis.

Artificial Intelligence-Generated Evidence

The BSA contains no explicit provision addressing the admissibility or authentication of AI-generated content. This is a significant legislative lacuna. Courts are already confronting evidence in the form of facial recognition identifications, predictive policing outputs, AI-transcribed recordings, and algorithmically generated financial analyses. The reliability of each of these requires an assessment of the algorithm's accuracy, the quality of the training data, the circumstances of application, and the potential for bias considerations that the BSA's general framework for expert evidence under Section 45 is poorly equipped to address.[19]

Deepfake technology presents a particular challenge: AI-generated audio or video evidence may be forensically indistinguishable from authentic recordings without highly sophisticated analysis. In jurisdictions such as California, the admissibility of manipulated media evidence in criminal proceedings has been addressed by specific legislation.[20]

Self-Incrimination and Compelled Production of Electronic Records

The Supreme Court in Selvi v. State of Karnataka held that the compelled administration of narco-analysis, brain mapping, and polygraph tests violates Article 20(3). The same logic potentially applies to compelling an accused to decrypt encrypted devices or provide biometric access (fingerprint or face recognition) to electronic devices.[21]

The BSA does not explicitly address this question. Section 94 permits courts to compel production of documents and electronic records, but its application to password-protected or encrypted devices and the constitutional implications thereof remains unresolved. This mirrors the live debate in the United States between the 'foregone conclusion' doctrine and the Fifth Amendment right against self-incrimination in the context of device decryption.[22]

Cloud-Stored Data and Cross-Border Evidence

A growing proportion of digital evidence resides in cloud infrastructure operated by foreign

[19] Rahul Sagar, 'AI-Generated Evidence and the Law: Challenges for Indian Courts' (2024) 14(1) Indian Journal of Law and Technology 78, pp. 82-95.
[20] California Assembly Bill No. 602 (2019) on the regulation of digital forgeries (deepfakes) as evidence in legal proceedings.
[21] Selvi v. State of Karnataka, (2010) 7 SCC 263 at para 190: compelling the accused to provide fingerprints or iris scan may be treated differently from compelling oral communications.
[22] In Re: Grand Jury, 21-4 (3rd Cir, 2022) (US Court of Appeals on the Fifth Amendment and device decryption); see also Orin S. Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106(4) Georgetown Law Journal 989.

entities outside Indian jurisdiction. The Mutual Legal Assistance Treaty (MLAT) framework for obtaining such evidence is notoriously slow, often taking two to three years to yield results. The BSA does not address this challenge, which is a major practical impediment to digital evidence collection in serious crimes including cybercrime, terrorism, and organized crime.[23]

DISCUSSION

Advances in the BSA Framework

The BSA makes several advances over the Indian Evidence Act's electronic evidence framework. The clearer articulation of the certificate requirement, the provisions for court-directed production, the expanded definition of electronic records to include data stored in any electromagnetic form, and the recognition of the evidentiary status of electronic contracts and digital signatures collectively modernize India's evidence law. The BSA's alignment with the Information Technology Act, 2000 and the Data Protection architecture represented by the Digital Personal Data Protection Act, 2023 creates a more coherent ecosystem for digital evidence.

Persistent and New Challenges

However, the BSA's silence on AI-generated evidence, its inadequate treatment of encrypted communications and device-extracted records, and the unresolved constitutional questions around compelled decryption are significant weaknesses. The fundamental problem is that legislation designed to last for decades is being tested against a technology environment that is transforming on a timescale of months. The BSA's framework is already, at the time of its enactment, struggling to accommodate the evidentiary implications of large language models, generative AI, and immersive synthetic media.

The epistemological challenge is particularly acute. Courts are trained and equipped to evaluate human testimony and documentary evidence. Electronic records, particularly those generated by complex algorithms or AI systems, introduce a qualitatively different evidentiary challenge: one that requires technical expertise that is rarely available in the criminal justice system and that interacts unpredictably with adversarial dynamics.

[23] Mutual Legal Assistance Treaty between India and the United States (2001); see also INTERPOL, Digital Forensics Working Group Report (2022) on cross-border digital evidence challenges.

Constitutional Fault Lines

The intersection of digital evidence law and constitutional rights will be the defining frontier of Indian evidence law over the next decade. The right to privacy established in Puttaswamy, the right against self-incrimination under Article 20(3), and the right to a fair trial under Article 21 all have significant implications for the admissibility of electronic evidence in criminal proceedings implications that the BSA does not systematically address.[24]

CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023 represents a significant but incomplete modernization of India's law of evidence in the domain of electronic records. While it addresses some of the interpretive difficulties generated by the Section 65B framework of the Indian Evidence Act, it leaves unresolved several critical questions regarding authentication standards, the admissibility of AI-generated evidence, the constitutional boundaries of compelled digital production, and the mechanisms for obtaining cloud-stored cross-border evidence.

The fundamental challenge facing India's electronic evidence law is one of temporal mismatch: legislation operates in a timeframe of years and decades, while digital technology evolves in a timeframe of months. The BSA, however well-intentioned, will require ongoing judicial creativity and legislative responsiveness to remain adequate to the evidentiary demands of criminal justice in the digital age. More fundamentally, the framework must be constitutionally robust protecting the rights of the accused against state power that has been exponentially amplified by digital surveillance and data-extraction capabilities.

RECOMMENDATIONS / SUGGESTIONS

On the basis of the foregoing analysis, the following recommendations are offered:

(i) Amendment of the BSA to introduce a specific provision addressing AI-generated evidence, requiring disclosure of the algorithm used, the training data, accuracy metrics, and the opportunity for expert challenge, as a condition of admissibility.

(ii) Enactment of a statutory standard for forensic tool certification and the validation of digital evidence extraction processes, as recommended by the UK Forensic Science Regulator.

[24] Justice K.S. Puttaswamy, supra note 14.

(iii) Legislative clarification or Supreme Court guidance on the application of Article 20(3) to compelled device decryption and biometric authentication, drawing on the 'foregone conclusion' doctrine and its limits.[25]

(iv) Amendment of the BSA to create a specific framework for cloud-stored data and cross-border electronic evidence, including a fast-track process for domestic courts to compel foreign cloud providers to produce data stored in Indian servers.

(v) Introduction of mandatory judicial training on the technical dimensions of digital evidence, given the complexity of evaluating electronic records, AI outputs, and forensic expert testimony.

(vi) Development of a comprehensive Electronic Evidence Code as a standalone legislation along the lines of Singapore's Electronic Transactions Act to provide a coherent, technology-specific framework that can be updated more responsively than a general evidence statute.

(vii) Recognition in the BSA of a 'digital chain of custody' requirement, mandating that law enforcement agencies document every step of digital evidence collection, extraction, and storage, with non-compliance having consequences for admissibility.

LIMITATIONS OF THE STUDY

The present study is subject to several limitations. First, as the BSA came into force in July 2024, judicial interpretation of its electronic evidence provisions remains nascent, and the paper relies primarily on textual analysis and extrapolation from the Section 65B jurisprudence. Second, the paper's technical analysis of AI and digital forensics issues is necessarily accessible rather than exhaustive, given the interdisciplinary nature of the inquiry. Third, the comparative analysis is limited to selected jurisdictions and does not engage with the full spectrum of approaches globally, particularly in Southeast Asia and Africa where comparable reform efforts are underway. Fourth, the paper does not undertake empirical analysis of how courts are actually evaluating digital evidence in criminal proceedings a gap that future field research should address.

[25] The 'foregone conclusion' doctrine, developed in Fisher v. United States, 425 US 391 (1976), holds that compelling production of documents does not violate the Fifth Amendment if their existence and authenticity are a 'foregone conclusion' to the prosecution.

SCOPE FOR FUTURE RESEARCH

Future research may productively focus on: empirical studies of judicial handling of electronic evidence in criminal courts under the BSA regime; the constitutional challenge to BSA provisions on compelled decryption and biometric access, which is likely to reach the Supreme Court in the near term; the development of judicial standards for evaluating AI-generated evidence in light of the National AI Strategy and the regulatory framework being developed by the Ministry of Electronics and Information Technology; the admissibility of evidence derived from surveillance operations under the Telecommunications Act, 2023 and its interaction with the BSA; and gender-sensitive analysis of the admissibility of intimate digital images and electronic communications in cases of sexual offences.

BIBLIOGRAPHY

Legislation

- The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023)
- The Indian Evidence Act, 1872 (Act 1 of 1872)
- The Information Technology Act, 2000 (Act 21 of 2000)
- The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)
- The Telecommunications Act, 2023
- Federal Rules of Evidence, United States (2023 edition)
- Police and Criminal Evidence Act, 1984 (UK)
- Criminal Justice Act, 2003 (UK)
- Electronic Transactions Act (Cap. 88), Singapore
- Regulation (EU) No. 910/2014 (eIDAS Regulation)

Case Law

- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
- Selvi v. State of Karnataka, (2010) 7 SCC 263
- State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600
- Tomaso Bruno v. State of U.P., (2015) 7 SCC 178

Books

- Duggal, Pavan, Cyber Law: The Indian Perspective (Saakshar Law Publications, New Delhi, 4th edn, 2022)
- Imwinkelried, Edward J., Evidentiary Foundations (Carolina Academic Press, 10th edn, 2020)
- Kamath, Nandan, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing, 6th edn, 2020)
- Kerr, Orin S., Computer Crime Law (West Academic Publishing, 5th edn, 2022)
- Mason, Stephen, Electronic Evidence (LexisNexis, 4th edn, 2017)
- Twining, William, Rethinking Evidence: Exploratory Essays (Cambridge University Press, 2nd edn, 2006)

Reports and Official Documents

- Internet Freedom Foundation, Analysis of the Bharatiya Sakshya Adhiniyam, 2023 (October 2023)
- Law Commission of India, 185th Report on Review of the Indian Evidence Act, 1872 (2003)
- National Institute of Standards and Technology (NIST), Digital Forensics Report Series (2023)
- Parliamentary Standing Committee on Home Affairs, Report on the Bharatiya Sakshya Adhiniyam, 2023 (November 2023)
- UK Forensic Science Regulator, Codes of Practice and Conduct for Forensic Science Providers (2023)

Journal Articles and Book Chapters

- Bhatia, Gautam, 'Privacy, Self-Incrimination and Digital Evidence in Indian Constitutional Law' (2024) 56(3) Journal of the Indian Law Institute 45
- Casey, Eoghan, 'Standards for Digital Evidence' (2011) 8(2) Digital Investigation 1
- Divan, Shyam, 'The Puttaswamy Judgment and Its Implications for Electronic Evidence Law' (2023) 35(2) National Law School of India Review 22
- Sagar, Rahul, 'AI-Generated Evidence and the Law: Challenges for Indian Courts' (2024) 14(1) Indian Journal of Law and Technology 78