IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

Cross-Border Data and its Admissibility Under the Bharatiya Sakshya Adhiniyam: Legal Challenges And Solutions

Vishnu Priyan V and Mr V. Mahalingam
Student
Assistant Professor
School of Law, SRM University, Chennai

Abstract: *The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (hereinafter "BSA") represents a momentous legislative reform in India's evidentiary framework, specifically with respect to digital and electronic records. While the BSA modernised the statutory landscape by elevating electronic records to the status of primary evidence and streamlining certification requirements, it has left conspicuously unresolved a range of complex issues pertaining to the admissibility of cross-border data in Indian courts. In an increasingly interconnected world, where evidence of crimes and civil disputes routinely resides on foreign servers, cloud platforms, and in the custody of multinational technology companies, the question of how such data is to be obtained, authenticated, and admitted before Indian tribunals acquires critical significance. This paper examines the existing framework under the BSA governing electronic evidence, evaluates the legal challenges posed by cross-border data in the Indian evidentiary context, and analyses the international mechanisms—particularly Mutual Legal Assistance Treaties (MLATs)—that mediate the process of procuring foreign-stored digital evidence. The paper further identifies the structural gaps in the BSA and proposes legislative and judicial solutions to ensure that the admissibility of cross-border data is placed on a sound, coherent footing. The analysis draws on landmark Supreme Court judgements, existing statutory provisions, and comparative international frameworks to offer a comprehensive critique and reform agenda*

Keywords: *Bharatiya Sakshya Adhiniyam*

I. INTRODUCTION

The Bharatiya Sakshya Adhiniyam, 2023, which came into force on July 1, 2024, replaces the Indian Evidence Act, 1872[1]—a colonial-era statute that governed evidentiary law in India for nearly one hundred and fifty years. The BSA introduces a series of progressive reforms, most significantly in the domain of electronic and digital evidence, thereby reflecting the legislative intent to align Indian law with the exigencies of a technology-driven society. The new statute, in its Sections 61 to 63,[2] fundamentally reconfigures the manner in which digital records are treated as evidence before courts of law.

However, the BSA, much like its predecessor, was primarily designed with a domestic evidentiary context in mind. The provisions governing electronic evidence under Section 63[3] presuppose, in large part, that the device or computer generating the electronic record is within Indian territorial jurisdiction and that the person competent to certify the record—being the person in charge of the device or an expert—is identifiable and accessible. This assumption breaks

[1]Indian Evidence Act, No. 1 of 1872 (India) (repealed 2023).
[2]Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 61 (India).
[3]Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(1) (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

down entirely when the evidence in question consists of cross-border data: emails stored on servers in the United States, social media communications hosted on Irish servers under EU data protection jurisdiction, financial transaction logs maintained by Singapore-based cloud service providers, or end-to-end encrypted messages on platforms governed by foreign laws.

The problem is not merely technical. It has far-reaching constitutional, sovereign, and jurisprudential dimensions. The right to privacy, recognised as a fundamental right by the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India,[4] intersects directly with the manner in which cross-border data is accessed and presented as evidence. The legality of obtaining evidence stored in foreign jurisdictions, the admissibility of such evidence once obtained, and the procedural requirements that must be satisfied under the BSA—all these issues demand urgent academic and legislative attention.

This paper proceed to analyse, in five parts: first, the framework for electronic evidence under the BSA; second, the concept and legal dimensions of cross-border data; third, the existing international mechanisms and their adequacy; fourth, the specific legal challenges posed under the BSA; and fifth, the proposed solutions to these challenges. The discussion is grounded in Indian statutory provisions, Supreme Court precedents, and comparative international law.

II. THE FRAMEWORK FOR ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

A. The Statutory Architecture

The BSA introduces a tripartite structure governing electronic evidence through Sections 61, 62, and 63. Section 61 provides that nothing in the Adhiniyam shall be used to deny the admissibility of an electronic or digital record as evidence on the ground that it is an electronic or digital record.[5] This provision constitutes a non-discrimination clause, ensuring that electronic records are not treated as inherently inferior to paper-based documentary evidence. Section 62 further provides that the contents of electronic records may be proved in accordance with Section 63.

Section 63(1) of the BSA is the cornerstone provision. It provides that any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory, which is produced by a computer or any communication device, shall be deemed to be also a document—and shall be admissible in any proceedings without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.[6] This provision significantly expands the scope of admissibility by including semiconductor memory and communication devices—a welcome clarification over the prior law.

Section 63(3) further broadens the definition of a computer or communication device to include networks of devices operating as a system,[7] thereby addressing the cloud computing scenario where data is processed across multiple servers. The BSA also mandates, under Section 63(4), that a certificate signed by the person in charge of the device and an expert must be submitted at the time of admission of the electronic record.[8] This dual-certification requirement—a notable departure from the old Section 65B(4) of the Indian Evidence Act which required only a single signatory in a responsible official position—is designed to enhance the accountability and credibility of electronic evidence.

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

[5] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 61 (India). See also PRS Legislative Research, The Bharatiya Sakshya Bill, 2023 (2023).

[7] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(3) (India).

[8] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4) (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

B. Key Judicial Antecedents

The evolution of the law relating to electronic evidence in India cannot be understood without reference to three landmark Supreme Court decisions. In Anvar P.V. v. P.K. Basheer & Ors.,[9] the Supreme Court held, for the first time with clarity, that Sections 65A and 65B of the Indian Evidence Act constitute a complete code for the admissibility of electronic records, and that no electronic record can be admitted as secondary evidence without the mandatory certificate under Section 65B(4). The Court overruled the contrary position taken in State (NCT of Delhi) v. Navjot Sandhu.[10]

Thereafter, a period of judicial uncertainty ensued. In Shafhi Mohammad v. State of Himachal Pradesh,[11] a division bench of the Supreme Court appeared to dilute the mandatory nature of the certificate, permitting waiver in the interests of justice where a party was not in possession of the device. This was held to be per incuriam and inconsistent with Anvar P.V. Similarly, the decision in Tomaso Bruno v. State of Uttar Pradesh,[12] which treated Sections 65A and 65B as merely procedural provisions, was also overruled.

The legal position was finally and definitively settled by the three-judge bench of the Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors.[13] The Court unequivocally held that the certificate under Section 65B(4) is a condition precedent to the admissibility of electronic evidence by way of secondary evidence.[14] It clarified that if the original electronic record itself is produced—for instance, by the owner of a laptop or mobile phone who steps into the witness box—no certificate is required. However, where the electronic record is part of a computer network or system that cannot be physically brought before the court, only the secondary evidence route with mandatory certification is available. The Court also invoked the Latin maxims lex non cogit ad impossibilia and impotentia excusat legem to provide relief in exceptional cases where the certificate could not be obtained despite best efforts.

These judicial precedents continue to be highly relevant under the BSA. The Rajya Sabha's Standing Committee on Home Affairs, in its Report No. 248 on the Bharatiya Sakshya Bill,[15] acknowledged the importance of the certification framework and recommended that the qualifications of experts to certify electronic evidence be clarified in the statute—a concern that the BSA ultimately did not fully resolve.

III. CROSS-BORDER DATA: CONCEPT AND LEGAL DIMENSIONS

A. What Constitutes Cross-Border Data?

Cross-border data, in the evidentiary context, refers to electronic records, digital communications, and data-sets that are physically stored in or transmitted through servers located outside the territorial jurisdiction of India. The definition of "electronic or digital records" under the BSA is broad enough to encompass emails, server logs, documents on computers, laptops, or smartphones, messages, websites, and voice mail messages stored on digital devices.[16] When such records are stored on foreign servers—as is routinely the case with Gmail accounts hosted in the United States, WhatsApp communications processed through servers in Ireland, or financial data maintained in Singapore—the question of how to obtain and admit them as evidence in Indian courts arises with pressing urgency.

---

[9] Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473 (India).

[10] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India) (overruled by Anvar P.V. on the question of Section 65B certificate requirements).

[11] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 (India).

[12] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178 (India).

[13] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors., (2020) 7 SCC 1 (India).

[14] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors., (2020) 7 SCC 1, ¶ 59 (India).

[15] Standing Committee on Home Affairs, Rajya Sabha, Report No. 248, The Bharatiya Sakshya Bill, 2023 (Nov. 10, 2023) (India).

[16] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 2(d) (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

The sheer scale of the problem is enormous. With over 900 million internet users in India and the explosive growth of digital commerce, online communications, and cloud-based services, a vast proportion of electronically stored information (ESI) that is relevant to Indian legal proceedings resides on foreign servers. Cybercrime investigations, tax evasion prosecutions, fraud trials, and even matrimonial disputes increasingly require access to data held by Meta (Facebook and WhatsApp), Google, Microsoft, Apple, Amazon Web Services, and similar multinational technology companies domiciled in foreign jurisdictions.

B. The Interplay with the Right to Privacy

The Supreme Court's landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India[17] has a significant bearing on the manner in which cross-border data may be obtained and used in evidence. The Court, through a nine-judge constitutional bench, unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. Crucially, the Court articulated the concept of informational privacy—the right of individuals to control the access, use, and dissemination of personal data that pertains to them.[18]

The Court further established a three-fold test for any state-sanctioned intrusion into privacy: legality (the action must be authorised by law), legitimate state aim, and proportionality (the means must be necessary and least intrusive). When Indian law enforcement agencies seek to obtain electronic data stored on foreign servers—whether through formal MLAT requests or through informal direct requests to technology companies—the question whether such access satisfies the Puttaswamy test acquires a constitutional dimension. Any statutory provision or executive action facilitating cross-border data access must, therefore, be consistent with the fundamental right to privacy as interpreted by the Supreme Court.

C. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (hereinafter "DPDPA") provides additional regulatory context for cross-border data flows.[19] Section 16(1) of the DPDPA empowers the Central Government to restrict, by notification, the transfer of personal data to certain countries or territories outside India—a "blacklist" approach.[20] Unlike earlier drafts that contemplated a stricter "whitelist" model, the final statute permits transfers to all jurisdictions by default unless specifically restricted. The DPDPA also contains an exemption under Section 17(2)(a) for state agencies processing data for purposes including prevention, detection, investigation, or prosecution of offences under Indian law.[21]

This exemption is of considerable significance for the cross-border data admissibility question: it suggests that law enforcement agencies may transfer and receive data across borders in the context of criminal investigations without being subject to the usual consent-based framework of the DPDPA. However, the DPDPA remains silent on how such data, once received from abroad, is to satisfy the certification requirements under Section 63(4) of the BSA. This legislative lacuna is one of the central concerns of this paper.

[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 180(x) (India).
[19] Digital Personal Data Protection Act, No. 22 of 2023, § 16 (India).
[20] Digital Personal Data Protection Act, No. 22 of 2023, § 16(1) (India).
[21] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(a) (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

IV. INTERNATIONAL MECHANISMS FOR CROSS-BORDER DATA ACCESS

A. Mutual Legal Assistance Treaties (MLATs)

The primary international mechanism through which India obtains electronic evidence from foreign jurisdictions is the Mutual Legal Assistance Treaty framework. A MLAT is a bilateral treaty between two states that establishes procedures for gathering and exchanging evidence and other forms of legal assistance for criminal investigations and prosecutions.[22] As of 2019, India had entered into MLATs with forty-two countries,[23] including the United States, the United Kingdom, and various European nations.

The India-US MLAT is of particular importance given that the United States is home to several of the world's largest technology companies whose servers store vast amounts of data relevant to Indian legal proceedings. Under this treaty, an Indian law enforcement agency wishing to obtain user data from a US-based service provider must file an MLAT request with the Ministry of Home Affairs (MHA),[24] which then forwards the approved request to the Office of International Affairs (OIA) under the US Department of Justice. The OIA reviews the request and, if satisfied, forwards it to a federal court that may order production. The entire process is subject to the requirements of the US Electronic Communications Privacy Act (ECPA),[25] which requires satisfaction of a probable cause standard.

The MLAT process is widely criticised for being extraordinarily slow. By some estimates, the average time taken for India to receive data through the India-US MLAT is well over three years.[26] A global study found that worldwide, the average MLAT process takes at least ten months to complete. Given the ephemeral nature of digital evidence—which may be deleted, encrypted, or otherwise made inaccessible over time—such delays can be fatal to a prosecution. The capacity deficit of Indian agencies in framing MLAT requests that comply with US legal standards compound these delays.[27]

B. Letters Rogatory

Where no MLAT exists between India and the requested nation, the alternative mechanism is the issuance of Letters Rogatory—formal judicial requests issued by an Indian court seeking the assistance of a foreign court or authority in gathering evidence. Sections 105 to 112 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (hereinafter "BNSS") govern this process in India.[28] Letters Rogatory are available even in the absence of a bilateral treaty, based on an assurance of reciprocity. However, the process is generally regarded as even more time-consuming and unpredictable than the MLAT route, since its enforcement depends on the comity of courts rather than treaty obligations. Prosecutors typically resort to Letters Rogatory only as a last resort.

C. The Budapest Convention and India's Non-Accession

At the multilateral level, the Budapest Convention on Cybercrime[29] is the only international treaty that deals comprehensively with cross-border cooperation in the collection of electronic evidence for criminal offences. It

---

[22] Jus Corpus, Mutual Legal Assistance Treaty Between US and India: Retrieving Online Data (Nov. 27, 2022), https://www.juscorpus.com/mutual-legal-assistance-treaty-between-us-and-india-retrieving-online-data/.

[23] Carnegie Endowment for International Peace, Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options? (Nov. 2020), https://carnegieendowment.org/research/2020/11/cross-border-data-access-for-law-enforcement-what-are-indias-strategic-options.

[24] Ministry of Home Affairs, India, Letter No. 25106/17/2017, Procedure for MLAT Requests (Feb. 11, 2009) (India).

[25] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2523 (1986) (USA).

[26] DeBrae Kennedy-Mayo et al., India-US Data Sharing for Law Enforcement: Blueprint for Reforms, Observer Research Foundation (Jan. 17, 2019).

[27] Observer Research Foundation, India's Access to Criminal Evidence in the US: A Proposed Framework for an Executive Agreement (Apr. 10, 2023), https://www.orfonline.org/research/indias-access-to-criminal-evidence-in-the-us.

[28] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 105–112 (India) (Letters Rogatory provisions).

[29] Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (India is not a signatory).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

provides mutual assistance mechanisms between state parties that may supplement existing MLATs, and permits unilateral access to data—without the other party's authorisation—in two specific situations: for publicly available data, and for data accessible through a computer system in the requesting state with the lawful and voluntary consent of the person authorised to disclose it.

India is notably not a signatory to the Budapest Convention. This absence means that India cannot avail of the supplementary cooperation mechanisms that the Convention creates between its parties. Given the growing volume of cross-border data requests involving Indian law enforcement and the demonstrated inadequacy of the bilateral MLAT framework, scholars and policy-makers have increasingly urged India to accede to the Budapest Convention or to negotiate direct access agreements modelled on the US CLOUD Act framework.[30] The failure to do so remains a significant structural gap in India's cross-border data access architecture.

D. Direct Requests to Technology Companies

In practice, Indian law enforcement agencies and private litigants also make direct requests to multinational technology companies for user data, particularly non-content data such as subscriber information and metadata. Most major technology companies have established transparency processes and legal response teams to handle such requests. However, the legal basis for compliance with such requests—and the admissibility of data obtained through them—is fraught with uncertainty under Indian law. The ECPA in the United States prohibits US-based service providers from disclosing the content of electronic communications to foreign governments without complying with the formal MLAT or other treaty-based processes. Metadata and subscriber information are governed by a somewhat less strict regime.

V. LEGAL CHALLENGES TO THE ADMISSIBILITY OF CROSS-BORDER DATA UNDER THE BSA

A. The Certification Conundrum

The most immediate and practically significant legal challenge posed by cross-border data under the BSA concerns the certification requirement under Section 63(4).[31] The provision requires that a certificate be signed by the person in charge of the device and by an expert. Where the electronic record originates from a foreign server—say, email communications stored on Google's servers in the United States—the "person in charge" of the device is, in legal terms, an officer or employee of a foreign corporation subject to foreign law. Such persons are unlikely to voluntarily provide a certificate in the format prescribed by the BSA, particularly given the legal exposure this might create for them under foreign law.

The BSA does not address this problem at all. It provides no mechanism for obtaining the equivalent of a Section 63(4) certificate from a foreign custodian of data. Unlike the MLAT framework, which can compel the production of data through a court order in the foreign jurisdiction, there is no corresponding mechanism under the BSA—or indeed under any other Indian statute—to compel the issuance of a certificate by a foreign custodian. This is a critical lacuna. In the absence of a valid certificate, the cross-border data cannot be admitted as secondary evidence under Section 63, regardless of how probative it may be.[32]

The problem is compounded by the dual-certification requirement of Section 63(4) of the BSA, which requires both the person in charge and an expert. Even where the data is eventually obtained through the MLAT process, there is no guarantee that the foreign authority providing the data will furnish a certificate in the format mandated by the BSA. The data may arrive with certifications that comply with the law of the requested state but do not satisfy the formal

[30] Centre for Internet and Society (CIS), Cross Border Data-Sharing and India: A Study in Processes, Content and Capacity, https://cis-india.org/internet-governance/files/mlat-report.

[32] Mayank Khichar, The Evolving Enigma, Vidhi Centre for Legal Policy (July 8, 2025), https://vidhilegalpolicy.in/blog/the-evolving-enigma/.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

requirements of Section 63(4). The question of whether such foreign-law-compliant certifications can be equated to the BSA certificate is entirely unresolved.[33]

B. Chain of Custody and Integrity of Evidence

A second major legal challenge concerns the chain of custody of cross-border data. The integrity of electronic evidence is a prerequisite for its admissibility and probative value. In domestic cases, Indian courts have emphasised the need to establish the chain of custody of electronic records to prevent challenges on grounds of tampering or contamination.[34] When data traverses multiple jurisdictions, multiple platforms, and multiple custodians before reaching the Indian court, the chain of custody becomes extraordinarily difficult to establish.

The problem is not merely technical. The Bombay High Court, in a case involving data obtained from a foreign server without a formal treaty,[35] held that electronic evidence obtained from foreign servers must be subject to local laws in the country where it is stored, and that data obtained in violation of foreign laws would be inadmissible. This ruling underscores the potential for foreign-law violations to taint the admissibility of cross-border data in Indian courts. The BNSS, under Section 94,[36] grants enhanced powers to police to seize electronic devices and records, but these powers are territorially limited and cannot be exercised extraterritorially.

C. Jurisdictional Sovereignty and Conflict of Laws

At a deeper level, the admissibility of cross-border data implicates questions of jurisdictional sovereignty. The principle of territorial sovereignty holds that a state has exclusive jurisdiction over persons and property within its territory. When Indian courts purport to compel the production of data stored in foreign servers, or when Indian investigators access such data without the consent of the foreign state, there is a real risk of violating the latter's sovereignty.

The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, 1970,[37] provides a framework for cross-border evidence gathering in civil proceedings, but it does not extend to criminal matters. The United Nations Convention Against Transnational Organized Crime[38] requires states to provide each other with the widest degree of mutual legal assistance, but this obligation is mediated through the MLAT framework and does not create direct rights of access to foreign-stored evidence. In the absence of a treaty-based obligation, the unilateral seizure or access of foreign-stored evidence by Indian authorities would be legally problematic and may render such evidence inadmissible under the doctrine of comity.

D. The Expert Qualification Gap

A further challenge relates to the "expert" whose signature is required under Section 63(4) of the BSA. The BSA does not define who qualifies as an expert for the purpose of certifying electronic evidence. This ambiguity was identified by the Rajya Sabha Standing Committee[39] as a significant weakness. In the cross-border context, the problem is even more acute. If the expert is to be a person skilled in the examination of documents, as the BSA broadly contemplates, questions arise as to whether a foreign forensic expert—appointed under the laws of a foreign jurisdiction—can qualify as the requisite expert under the BSA.

---

[33] LexisNexis India, Decoding Bharatiya Sakshya Adhiniyam, 2023: Comparative Insights & Study with Indian Evidence Act, 1872 (Oct. 9, 2025), https://www.lexisnexis.com/blogs/in-legal/b/law/posts/decoding-bharatiya-sakshya-adhiniyam-2023-comparative-insights-study-with-indian-evidence-act-1872.

[34] Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke, (2015) 3 SCC 123, ¶ 16 (India).

[35] Virendra Khanna v. State of Karnataka, W.P. No. 11759 of 2020 (Kar. H.C. Mar. 12, 2021) (India).

[36] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 94 (India).

[37] Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 847 U.N.T.S. 231.

[38] United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209, art. 18(1).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

Equally significant is the shortage of qualified forensic science laboratories (FSLs) in India. As noted in legal scholarship, the BSA's reliance on expert certification presupposes institutional capacity and a sufficient pool of qualified experts, an assumption that may not hold good in many parts of the country.[40] In the cross-border context, where the complexity of the forensic analysis is likely to be higher, this infrastructure deficit becomes an even more pressing concern.

E. Privacy and the Proportionality Test

Any statutory framework authorising the collection and admission of cross-border data as evidence must also satisfy the proportionality test articulated in Puttaswamy.[41] The Supreme Court held that any restriction on the right to informational privacy must be sanctioned by law, pursue a legitimate state aim, and adopt means that are necessary and least intrusive. A law enforcement regime that permits broad and indiscriminate access to cross-border data—without adequate judicial oversight, purpose limitation, or data minimisation principles—would likely fail this constitutional test.

The current Indian framework for cross-border data access, which relies primarily on the executive-driven MLAT process without mandatory judicial authorisation, does not clearly satisfy the Puttaswamy proportionality standard. The DPDPA's exemption for law enforcement agencies under Section 17(2)(a)[42] may shield certain government activities from DPDPA compliance, but it does not insulate them from constitutional scrutiny under Article 21 as interpreted by the Supreme Court.

VI. PROPOSED SOLUTIONS

A. Legislative Amendments to the BSA

The most fundamental reform required is a legislative amendment to Section 63 of the BSA to address the cross-border data scenario explicitly. The amended provision should provide for an alternative certification mechanism where the custodian of the electronic record is a foreign entity: for instance, by permitting the use of a certificate issued by the competent authority of the requested state in accordance with MLAT or Letters Rogatory procedures, provided such certificate substantially complies with the informational requirements of Section 63(4). This approach is consistent with the principle articulated in Arjun Panditrao that the law should not demand the impossible—and it is plainly impossible for a foreign corporation to issue a certificate in the precise statutory form mandated by the BSA.[43]

The BSA should also be amended to prescribe the qualifications of experts authorised to certify electronic evidence, both domestic and foreign. This would resolve the expert qualification gap and ensure that foreign forensic experts whose reports accompany cross-border data can be recognised under the BSA framework. The Standing Committee's recommendation on this point[44] should be implemented without further delay.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, April 2026 Impact Factor: 8.2

B. Modernising the MLAT Framework

The MLAT framework requires urgent reform to address the problems of delay and procedural complexity that characterise the current process. India should negotiate updated MLATs—or MLAT supplements—with major data-hosting jurisdictions, particularly the United States, to incorporate faster electronic evidence request mechanisms, reduced timelines for compliance, and single-point contact systems. The Observer Research Foundation's blueprint for India-US data sharing reforms[45] provides a detailed roadmap for such negotiations, including the potential for a bilateral executive agreement under the US CLOUD Act framework that would enable Indian authorities to make direct data requests to US technology companies in serious criminal cases, subject to appropriate privacy safeguards.

C. Accession to the Budapest Convention

India should seriously consider acceding to the Budapest Convention on Cybercrime.[46] Accession would provide India with access to a multilateral cooperative framework for electronic evidence gathering, reduce the burden on bilateral MLAT processes, and place India's law enforcement agencies in a stronger legal position when dealing with data stored in signatory states. The Convention's provisions on expedited preservation of stored computer data, disclosure of preserved data, and real-time collection of traffic data would significantly augment India's cross-border data access capabilities.

D. Judicial Mechanisms and Presumptions

In the absence of comprehensive legislative reform, Indian courts can play a significant role in bridging the admissibility gap through creative judicial interpretation. Courts could, drawing on the Latin maxims invoked in Arjun Panditrao,[47] adopt a flexible approach to the certification requirement under Section 63(4) in cases involving cross-border data, treating foreign-law-compliant certifications as substantially compliant with the BSA where the data has been obtained through an MLAT or Letters Rogatory process. Such an approach would be consistent with the principle of comity, which requires Indian courts to give effect to the acts of foreign governments performed within their own territory.

Courts might also consider developing evidentiary presumptions—akin to those in Sections 81 to 90 of the BSA—for electronic records obtained through formal international legal assistance channels. A presumption of authenticity for such records, rebuttable on proof of specific grounds (such as tampering or violation of the applicable foreign law), would go a long way in resolving the practical admissibility problems posed by cross-border data.[48]

E. Strengthening Institutional Capacity

Finally, any solution to the cross-border data admissibility problem must be accompanied by significant investment in institutional capacity. The MHA's internal security division, which handles MLAT requests, must be strengthened with dedicated personnel trained in international law and digital forensics. Indian FSLs must be adequately funded and equipped to handle the complex forensic analysis that cross-border electronic evidence typically requires. The Supreme Court, in William Stephen v. State of Tamil Nadu,[49] emphasised the importance of proper training for police officers in handling digital evidence—a principle that applies with even greater force to the cross-border context.

---

[48]Drishti Judiciary, Electronic Evidence Under Bhartiya Sakshya Adhiniyam, 2023 (July 16, 2024), https://www.drishtijudiciary.com/bharatiya-sakshya-adhiniyam-&-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023.

[49]William Stephen v. State of Tamil Nadu, (2020) (referencing mandatory police training for electronic evidence – cited in Law.asia analysis of BSA).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, April 2026
Impact Factor: 8.2

VII. CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023 represents a landmark legislative development in India's evidentiary history, and its treatment of electronic evidence as primary evidence is to be commended as a bold step towards modernity. However, in failing to address the admissibility of cross-border data, the BSA has left a significant and consequential gap in India's evidentiary architecture. As the boundaries between domestic and international crime increasingly blur—as cybercriminals, financial fraudsters, and other offenders exploit the inherently borderless character of digital communications—the inability of Indian courts to seamlessly admit cross-border data as evidence will have serious ramifications for the administration of justice.

The legal challenges identified in this paper—the certification conundrum, the chain of custody problem, the jurisdictional sovereignty question, the expert qualification gap, and the constitutional privacy constraints—are not merely theoretical. They are live issues that arise, or will arise, in courtrooms across India as prosecutors and litigants seek to rely on evidence stored on foreign servers. The solutions proposed—legislative amendment of Section 63, reform of the MLAT framework, accession to the Budapest Convention, judicial creativity in presumptions of authenticity, and investment in institutional capacity—are complementary rather than alternative, and must be pursued simultaneously.

The BSA, if amended and supplemented along the lines suggested in this paper, has the potential to provide a comprehensive and constitutionally sound framework for the admissibility of cross-border data in Indian courts. The challenge for Indian legislatures, courts, and policymakers is to rise to this occasion—before the evidentiary lacunae identified herein cause serious miscarriages of justice in cases where cross-border digital evidence is crucial to the truth-seeking function of the judicial process.