Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Cross-Border Access to Electronic Evidence: Jurisdictional Challenges, The Budapest Convention, And Admissibility Under Section 63 Of The Bharatiya Sakshya Adhiniyam, 2023

Dr. Sunandini[1], Devashees Dev Kumar Verma[2], Manoj Kumar[3]

[1,2,3]Amity University Uttar Pradesh, Noida

Abstract

Distributed cloud computing, data sharding, and end-to-end encryption have severed the traditional Westphalian nexus between physical territory and criminal evidence. In transnational offences—ranging from cyber-enabled financial fraud and ransomware to terror financing—crucial digital records routinely reside on foreign servers controlled by multinational Communication Service Providers (CSPs). Indian law enforcement confronts an acute structural friction: urgent investigative needs collide with protracted Mutual Legal Assistance Treaty (MLAT) procedures, foreign blocking statutes, and conflicting data protection mandates. This article examines the triadic legal framework governing cross-border electronic evidence from an Indian perspective. First, it analyses the jurisdictional deadlock created by data un-territoriality alongside unilateral mechanisms such as the United States CLOUD Act and the European Union e-Evidence Regulation. Second, it evaluates international treaty architectures, contrasting the Council of Europe's Budapest Convention on Cybercrime (2001) and its Second Additional Protocol (2022) with India's non-signatory reservations over Article 32(b) and its pivot toward the United Nations Convention against Cybercrime (2024). Third, it undertakes a doctrinal critique of Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), demonstrating how its mandatory two-part Schedule certificate and hash verification create severe evidentiary hurdles when foreign CSPs refuse to execute Indian statutory forms, and proposes targeted statutory, diplomatic, and forensic reforms.

Keywords: Electronic Evidence, Cross-Border Jurisdiction, Section 63 Bharatiya Sakshya Adhiniyam 2023, Budapest Convention, UN Cybercrime Convention, US CLOUD Act, Mutual Legal Assistance.

1. Introduction

Modern criminal investigations have shifted decisively from physical crime scenes to volatile digital trails. Whether investigating ransomware syndicates, cross-border financial fraud, child sexual exploitation, or terror financing coordinated over encrypted platforms, law enforcement relies on electronic data that transcends national frontiers. A complainant may reside in Noida, the perpetrator in another Indian state, the cloud infrastructure in Ireland, and the corporate controller in the United States. While data can be replicated, fragmented, or erased instantaneously without crossing a physical border, criminal enforcement jurisdiction remains strictly anchored to state territory.

This asymmetry creates a dual risk. Protracted evidence-gathering enables automatic log overwriting and deliberate spoliation, crippling prosecutions; conversely, unregulated cross-border data transfers erode individual privacy and due process safeguards. The central legal question is therefore not whether states must cooperate, but on what jurisdictional basis, through which procedural channel, and in what evidentiary format foreign-hosted electronic records can be admitted before domestic trial courts.

With the enforcement of the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) on 1 July 2024, India overhauled its colonial-era criminal evidence regime. Section 63 of the BSA, replacing Section 65B of the Indian Evidence Act, 1872 (IEA), retains the mandatory certification requirement for secondary electronic records while tightening compliance through a prescribed two-part Schedule form, dual signatories, and mandatory cryptographic hash disclosure. However, Section 63 was drafted primarily with domestic custodians in mind. Employing a doctrinal and comparative methodology—examining Indian statutes, Supreme Court jurisprudence, the Budapest Convention, the United Nations Convention against Cybercrime, the US CLOUD Act, and the EU e-Evidence Regulation—this article tests a focused hypothesis: while Section 63 modernises domestic digital forensics, its rigid application to foreign-hosted records without a treaty-compliant authentication exception risks excluding vital evidence in transnational cybercrime prosecutions.

2. Jurisdictional Paradoxes in Cloud Architecture

A. Westphalian Territoriality Versus Data Sharding

Public international law distinguishes between prescriptive, adjudicative, and enforcement jurisdiction. As affirmed in S.S. Lotus (France v. Turkey, 1927), enforcement jurisdiction is strictly territorial: state officials cannot exercise coercive investigative powers within another sovereign's territory absent consent, typically routed through a Mutual Legal Assistance Treaty (MLAT). Cloud computing disrupts this territorial premise. To optimise latency and redundancy, multinational Communication Service Providers (CSPs) dynamically shard user data across global data centres—storing account metadata in Dublin, attachments in Singapore, and rotating backups across Oregon and Frankfurt within milliseconds. Anchoring criminal jurisdiction to server geography produces arbitrary outcomes: a purely domestic offence committed in India using foreign cloud platforms becomes trapped in an international jurisdictional deadlock.

B. Competing Jurisdictional Theories

Courts, legislatures, and scholars have advanced four competing frameworks to resolve data un-territoriality:

1. Data-Location Theory: Enforcement authority attaches to the physical location of the server. Accessing overseas servers is treated as an extraterritorial intrusion into the host state's sovereignty—a position central to Microsoft's challenge in United States v. Microsoft Corp. (2018).

2. Corporate-Control Theory: Jurisdiction follows the corporate entity possessing possession, custody, or control over the data, irrespective of server geography. While Section 94 of the BNSS and Section 75 of the Information Technology Act, 2000 (IT Act) reflect elements of this approach, multinational CSPs

routinely vest data control in foreign parent corporations while restricting Indian subsidiaries to marketing or local support.

3. Target-Based Nexus Theory: Advocated by scholars such as Jennifer Daskal, this model prioritises the territorial nexus of the victim, perpetrator, and criminal harm over arbitrary server locations, provided domestic warrants satisfy robust substantive safeguards.

4. Loss-of-Location Theory: Where anonymisation tools (such as Tor or layered VPNs) obscure server geography, jurisdictions like Belgium (in the Yahoo! and Skype rulings) and Germany assert authority to compel any provider offering services within their market to disclose user data.

C. The MLAT Bottleneck, Blocking Statutes, and Unilateral Fast-Tracks

Although India maintains MLATs with over forty-five jurisdictions and designates the Ministry of Home Affairs (MHA) as its Central Authority under Section 112 of the BNSS, the treaty mechanism is structurally ill-suited to digital volatility. A typical MLAT request traverses state police, state home departments, the MHA, diplomatic channels, the US Department of Justice, a federal prosecutor, and a magistrate—frequently consuming ten to twenty-four months. Requests frequently fail due to divergent evidentiary thresholds, notably the American 'probable cause' requirement, or lack of dual criminality in speech-related offences.

Compounding these delays are foreign blocking statutes. Under the US Stored Communications Act (18 U.S.C. § 2702), American CSPs are prohibited from disclosing stored communications content to foreign governments absent a US judicial warrant, though basic subscriber and IP logs may be disclosed voluntarily. Similarly, Article 48 of the European Union General Data Protection Regulation (GDPR) bars transfers pursuant to foreign orders unless anchored in an international agreement. To bypass MLAT paralysis, Western jurisdictions enacted unilateral and regional fast-tracks: the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018 (18 U.S.C. § 2713) compels US-based providers to produce controlled data globally and authorises bilateral executive agreements (concluded with the UK, Australia, and Canada) lifting blocking restrictions; meanwhile, the EU e-Evidence Regulation (applicable from August 2026) empowers judicial authorities to issue European Production Orders directly to providers across Member States with a ten-day compliance window (eight hours in emergencies). Lacking a CLOUD Act agreement, Indian agencies remain excluded from expedited content disclosure.

3. International Treaty Frameworks: Budapest and Beyond

A. The Budapest Convention (2001) and Second Additional Protocol (2022)

The Council of Europe’s Convention on Cybercrime (Budapest Convention, 2001; in force 2004), comprising 84 States Parties by late 2026, remains the primary multilateral instrument harmonising substantive cyber offences, procedural powers, and international cooperation. For cross-border evidence, four provisions are pivotal: Article 18 (domestic production orders over controlled data and subscriber information), Articles 29 and 30 (expedited preservation of volatile data for up to ninety days pending formal MLAT transmission), Article 35 (a 24/7 operational point-of-contact network), and Article 32(b), which permits unilateral trans-border access to stored computer data without host-state authorisation where the lawful controller consents.

To address cloud delays, the Council of Europe adopted the Second Additional Protocol (opened for signature in May 2022, attracting over fifty-two signatories through 2026). Article 7 empowers competent authorities to transmit binding production orders directly to service providers in another Party's territory for subscriber information—bypassing central authorities—subject to optional host-state notification and refusal safeguards, alongside Article 8 (expedited production of subscriber and traffic data) and Article 10 (emergency mutual assistance).

B. India's Non-Signatory Dilemma and the UN Cybercrime Convention

For over two decades, India declined to accede to the Budapest Convention on three principal grounds: (i) exclusion from its initial drafting as a regional European treaty; (ii) sovereignty objections to Article 32(b), fearing foreign agencies could access data hosted in India via foreign corporate consent without notifying New Delhi; and (iii) historical absence of comprehensive domestic data protection legislation meeting European adequacy standards.

Instead, India championed a universal multilateral instrument under United Nations auspices. Adopted by the UN General Assembly on 24 December 2024 and opened for signature in October 2025 (entering into force ninety days after its fortieth ratification), the United Nations Convention against Cybercrime—which India has signed—incorporates a 24/7 network, expedited preservation, and streamlined MLAT procedures while omitting unilateral trans-border access akin to Article 32(b) and reaffirming sovereign equality. However, until universal ratifications mature, Indian investigators operate in an institutional interregnum.

4. Admissibility Under Section 63 Of The BSA, 2023

A. Statutory Evolution and Core Architecture

For nearly twenty-four years following the IT Act, 2000, Sections 65A and 65B of the IEA governed electronic records. Borrowed from Section 5 of the repealed UK Civil Evidence Act, 1968, Section 65B referred narrowly to 'optical or magnetic media'—creating interpretive friction regarding solid-state drives, smartphones, and distributed cloud servers—and prescribed no standardised certificate format, resulting in mechanical affidavits.

The BSA modernises this framework. Section 2(1)(d) expands 'document' to encompass electronic and digital records, including emails, server logs, smartphones, websites, and location data. Explanations 4 to 7 of Section 57 clarify when electronic outputs constitute primary evidence, while Section 61 bars rejection solely on electronic form. Section 63(1)–(5) replaces Section 65B with five structural modifications:

1. Technological Neutrality (Section 63(1)): Explicitly covers 'semiconductor memory' and 'any communication device', eliminating ambiguity over flash storage, mobile extractions, and cloud terminals.

2. Distributed Network Aggregation (Section 63(3)): Treats interconnected computers and distributed cloud networks operating in combination as a single computer.

3. Mandatory Contemporaneous Certification (Section 63(4)): Mandates submission of a certificate along with every electronic record tendered in evidence, omitting the diluted 'best of knowledge and belief' qualifier.

4. Dual-Part Schedule Certificate: Requires execution in the statutory format prescribed in the Schedule, signed jointly by the person in charge of the device or management of the relevant activities (Part A) and an expert (Part B).

5. Mandatory Hash Value Disclosure: Obliges signatories to identify the source medium and specify the cryptographic hash value alongside the algorithm applied (such as SHA-256 or SHA-512), establishing mathematical proof of integrity.

B. Judicial Trajectory: From Anvar P.V. to Pune Bar Association (2026)

Indian jurisprudence under Section 65B oscillated before crystallising into strict compliance. After State (NCT of Delhi) v. Navjot Sandhu (2005) permitted secondary electronic records without certification, a three-judge bench in Anvar P.V. v. P.K. Basheer (2014) overruled it, holding Section 65B to be a complete code where secondary copies are inadmissible absent a statutory certificate, though primary devices require none. Following a brief relaxation in Shafhi Mohammad v. State of Himachal Pradesh (2018), a Constitution Bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) reaffirmed Anvar P.V., while carving out a narrow exception under the doctrine of impossibility (lex non cogit ad impossibilia): where a party exhausts all legal remedies to obtain a certificate from an uncooperative third-party custodian, the court may summon the record and excuse strict compliance.

The constitutionality of Section 63(4)'s heightened rigour was tested in Pune Bar Association v. Union of India (Supreme Court, 8 July 2026), following a Madras High Court ruling (R. v. B., 2024) restricting Part B certification to examiners notified under Section 79A of the IT Act. Upholding Section 63(4), a three-judge bench led by Chief Justice Surya Kant affirmed that mandatory hash verification functions as an indispensable 'electronic fingerprint' against deepfakes and digital tampering, thereby cementing dual-part certification as a strict threshold condition.

5. The Collision Point: Admitting Foreign-Hosted Records

A. Structural Friction Under Section 63(4)

Consider a cyber-fraud investigation conducted by the Central Bureau of Investigation (CBI) or Noida Cyber Police involving a fraudulent platform hosted on Amazon Web Services in Virginia and operated via Gmail and WhatsApp accounts. Pursuant to an MLAT request or emergency disclosure portal, Google or Meta transmits a compressed archive containing subscriber logs and communications accompanied by a SHA-256 hash. When tendered before a trial court, four structural obstacles arise under Section 63:

1. Refusal to Execute Indian Statutory Forms: US-based CSPs routinely issue declarations under 28 U.S.C. § 1746 and Federal Rule of Evidence 902(11) signed by a records custodian certifying automated business-record generation and archive hashes, but systematically refuse to execute the Indian Schedule form on grounds of extraterritorial non-applicability and corporate liability.

2. Inability to Satisfy Part A: Part A requires certification that the originating server operated properly under the signatory's lawful control. An Indian investigating officer who merely downloads an archive from a law enforcement portal lacks personal knowledge or control over servers in Oregon or Dublin, and can truthfully certify only the local receiving terminal.

3. Forensic Scope Limits Under Part B: Part B requires an expert to verify the record's integrity and hash value. While an Indian forensic examiner can compute the hash upon download, the examiner cannot audit the foreign CSP's extraction pipeline.

4. Confrontation and Cross-Examination Hurdles: Summoning a California-based custodian to testify in an Indian trial is practically unfeasible, forcing reliance on video-conferencing under Section 308 of the BNSS or statutory presumptions.

B. Interpretive and Procedural Pathways

To prevent routine exclusion of authentic foreign evidence, prosecutors and trial courts must deploy four cumulative pathways: (i) invoking Section 89 of the BSA (presumption as to certified copies of foreign judicial and official records authenticated by Indian diplomatic or consular officers) alongside the Arjun Panditrao impossibility doctrine; (ii) maintaining an exhaustive documentary trail of Section 94 BNSS notices, portal requests, and MHA MLAT transmissions alongside the CSP's written refusal to establish impossibility; (iii) executing two-stage hash verification—preserving the CSP's origin hash at the moment of portal download under Part A and generating a matching write-protected forensic hash in India under Part B; and (iv) seizing suspects' local endpoints under audio-video recording pursuant to Section 105 of the BNSS so that cached communications may be tendered as primary evidence under Explanation 4 to Section 57 of the BSA.

6. Comparative Matrix of Transnational Frameworks

Table 1 synthesises the jurisdictional basis, acquisition mechanisms, evidentiary authentication rules, and operational bottlenecks for India across the four governing legal regimes.

Dimension	Budapest Convention + 2nd Protocol	UN Cybercrime Convention (2024)	US CLOUD Act (2018)	Section 63, BSA (India)
Nature & Status	Binding multilateral treaty (84 Parties by late 2026); 2nd Protocol operationalising.	Global UN treaty; signed by India (2025), awaiting 40 ratifications.	US domestic statute + bilateral executive agreements (UK, Australia, Canada).	Indian domestic admissibility code governing electronic evidence (in force July 2024).
Jurisdictional Basis	Territoriality, domestic data control (Art. 18), and consent-based access (Art. 32(b)).	Strict sovereign equality and territoriality; excludes unilateral Art. 32(b) access.	Corporate possession, custody, or control regardless of server location.	Lex fori admissibility rule applicable to all records tendered in Indian courts.
Acquisition	24/7 network, 90-	24/7 network,	US judicial	No extraterritorial

Channel	day preservation (Arts. 29–30), direct subscriber orders (Art. 7).	expedited preservation, and streamlined MLAT channels.	warrants; executive agreements lift SCA blocking bars for partners.	compulsion; relies on BNSS § 94 and MHA MLAT channels.
Authentication & Bottleneck	Left to domestic law; India remains a non-signatory due to Art. 32(b) concerns.	Calls for mutual authentication assistance; not yet in force.	US FRE 902(11) & § 1746 hash declarations; India lacks an executive agreement.	Mandatory Part A & Part B Schedule certificate + hash; foreign CSPs refuse to sign.

7. Recommendations and Conclusion

Cloud architecture has rendered rigid territorial enforcement obsolete, trapping Indian criminal justice between slow international assistance and stringent domestic evidentiary formalities. While Section 63 of the BSA strengthens forensic reliability through dual certification and cryptographic hashing, mechanical insistence on its Schedule format for foreign-hosted records risks insulating transnational cybercriminals behind procedural technicalities. Five targeted reforms can resolve this impasse:

1. Enact a Statutory Proviso to Section 63(4): Parliament should amend Section 63(4) to provide that where electronic records are received from a foreign CSP or authority through an MLAT, executive agreement, or international convention, a business-record declaration valid under the transmitting state's law (such as 28 U.S.C. § 1746) embedding a SHA-256 or stronger hash shall satisfy Part A, when paired with a Part B certificate executed by an Indian forensic expert upon receipt.

2. Negotiate a Bilateral US CLOUD Act Agreement: Given that over three-quarters of Indian law enforcement data requests target US-headquartered providers, the Ministries of External Affairs and Home Affairs should prioritise a bilateral CLOUD Act executive agreement, leveraging the Digital Personal Data Protection Act, 2023 and judicial oversight under the BNSS to eliminate twelve-to-twenty-four-month MLAT delays.

3. Operationalise the UN Cybercrime Convention: India should expedite ratification of the UN Convention against Cybercrime and establish a dedicated 24/7 National Electronic Evidence Cooperation Desk within the Indian Cyber Crime Coordination Centre (I4C) to operationalise expedited preservation from the treaty's entry into force.

4. Issue Standard Operating Procedures for Chain of Custody: The Bureau of Police Research and Development and I4C should issue binding protocols requiring investigators to record origin hashes at download, generate matching Indian Part B hashes, and file formal records of foreign CSP refusals to trigger the Arjun Panditrao impossibility exception.

5. Expand Section 79A Forensic Capacity and Judicial Training: In alignment with Pune Bar Association (2026), the Union Government should accelerate the notification of regional forensic laboratories under Section 79A of the IT Act and institute specialised judicial training at the National and State Judicial Academies on cloud architecture and cross-border authentication.

Ultimately, effective transnational cybercrime prosecution requires harmonising investigative speed with forensic integrity. By pairing diplomatic modernisation with calibrated evidentiary flexibility under Section 63 of the BSA, India can safeguard both sovereign due process and courtroom admissibility in a borderless digital era.

Select Bibliography and Authorities

1. **Indian Statutes:** Bharatiya Sakshya Adhiniyam, 2023 (§§ 2(1)(d), 57, 61, 63, 89, Schedule); Bharatiya Nagarik Suraksha Sanhita, 2023 (§§ 94, 105, 112, 308); Indian Evidence Act, 1872 (§§ 65A, 65B); Information Technology Act, 2000 (§§ 75, 79A); Digital Personal Data Protection Act, 2023.
2. **International Instruments & Foreign Legislation:** Council of Europe Convention on Cybercrime (2001) & Second Additional Protocol (2022); United Nations Convention against Cybercrime (adopted Dec. 2024, opened Oct. 2025); Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018, 18 U.S.C. § 2713; Stored Communications Act, 18 U.S.C. § 2702; Regulation (EU) 2023/1543 (e-Evidence Regulation).
3. **Judicial Decisions:** S.S. Lotus (France v. Turkey), 1927 P.C.I.J. (ser. A) No. 10; United States v. Microsoft Corp., 584 U.S. 236 (2018); State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 S.C.C. 600; Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473; Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 S.C.C. 801; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1; R. v. B., 2024 SCC OnLine Mad 6052; Pune Bar Association v. Union of India, Supreme Court of India (8 July 2026).
4. **Scholarly Literature:** Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale Law Journal 326; Jennifer Daskal, 'Borders and Bits' (2018) 71 Vanderbilt Law Review 179; Andrew Keane Woods, 'Against Data Exceptionalism' (2016) 68 Stanford Law Review 729; Dan Jerker B. Svantesson, Solving the Internet Jurisdiction Puzzle (OUP 2017).