



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## Smart Contracts, AI-Generated Evidence, and the Challenge of International Arbitration: An Analysis of India's Legal Framework

~ *Pari Shreya Maligonda*

### INTRODUCTION

---

The rise in the application of artificial intelligence and blockchain technologies has led to significant changes in the way commercial disputes are managed. Smart contracts refer to automated digital agreements that exist on the blockchain system and are automatically activated upon meeting certain stipulated conditions. Currently, smart contracts are extensively utilized in international business dealings. On the other hand, documents generated through artificial intelligence, predictive analytics, and machine learning are becoming more common in arbitral proceedings. Such advancements have created legal issues, considering the laws were formulated long before such technologies existed.

The principal legislation applicable to arbitration in India is the Arbitration and Conciliation Act, 1996 (A&C Act). In 2015 and 2019, the A&C Act underwent modifications to increase efficiency and ensure compliance with international standards. The Indian Evidence Act, 1872 (IEA) and the Information Technology Act, 2000 (IT Act) are the relevant statutes in

dealing with issues related to electronic evidence. The recently introduced Digital Personal Data Protection Act, 2023 (DPDP Act) has prescribed regulations pertaining to consent and personal data protection in relation to sharing of documents in international arbitrations. However, none of these statutes regulate the area of smart contract and/or AI evidence.

This article is split into five parts. Part II considers whether smart contracts can satisfy the legal requirements for an arbitration agreement under Section 7 of the A&C Act. Part III covers the admissibility of AI generated documents as evidence under Indian law. Part IV discusses the impact of the DPDP Act on cross-border sharing of documents in arbitration. Part V compares India's legal framework with international standards like the IBA Rules on the Taking of Evidence in International Arbitration and the GDPR. Finally, Part VI addresses existing gaps in law and suggests reforms.

## **EXAMINING SMART CONTRACTS UNDER THE ARBITRATION AND CONCILIATION ACT, 1996**

---

### ***A. The Statutory Framework***

Section 7 of Arbitration and Conciliation Act, 1996 defines arbitration agreement as an agreement between the parties to submit to arbitration present or future disputes. It also requires that the agreement be in writing. An agreement is "in writing" if evidenced by: (a) a signed writing; or (b) the transmission of a signed writing by mail, facsimile or electronic means [1]. This definition was amended in 2015 to expressly include electronic communications in recognition of the increased use of digital transactions.

Whether a smart contract, which is computer code on a blockchain, may meet Section 7 standards is a crucial legal question. Any data or information created, stored, received, or sent electronically is considered an "electronic record" under the Information Technology Act of 2000 [2]. Furthermore, according to Section 4 of the IT Act, information that is available in an electronic format that can be accessed and consulted at a later time satisfies any legal need that information be in writing.

When read together, these provisions suggest that a smart contract recorded on a blockchain can be treated as a valid electronic record in writing under Indian law.

### ***B. Mutuality, Consent and the Autonomy Problem***

But merely meeting the electronic writing criterion is insufficient. In order for arbitration to be used to settle conflicts, both parties must sincerely consent, as required by Section 7. Smart contracts are frequently developed by developers or online platforms and approved by users via click-wrap or digital wallet signatures. A thorough comprehension of the arbitration clause may not always be reflected in such acceptance [3]. Indian courts have consistently ruled that the parties must be sufficiently informed of an arbitration clause and that their consent must be explicit and well-informed [4].

The Supreme Court ruled in *Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.* that electronic communications might demonstrate an arbitration agreement if they make it evident that the parties want to arbitrate disputes [5]. According to this theory, the legal requirement would probably be satisfied by a smart contract that has an arbitration clause in easily understandable English at the time of execution. However, it becomes far more challenging to show legitimate permission if the provision is concealed within complicated computer code that is incomprehensible to regular users.

### **C. Specific Enforceability and Judicial Attitudes**

The independent enforceability of an arbitration clause in a smart contract has not yet been directly decided by Indian courts. Nonetheless, where blockchain-based recordings meet Section 65B of the Indian Evidence Act's certification standards, courts have recognized them as legitimate electronic evidence [6].

Furthermore, the Delhi High Court has demonstrated a pragmatic and technologically advanced approach to blockchain-related issues by granting interim relief in cases involving bitcoin assets under Section 9 of the Arbitration and Conciliation Act [7].

Even with this constructive strategy, there are still practical challenges. Parties requesting the appointment of an arbitrator are often required by Section 11 of the A&C Act to present copies of the arbitration agreement to the court. obtaining legible and correctly authenticated documents in cases where the agreement is only present as on-chain blockchain code.

## **ADMISSIBILITY OF AI-GENERATED DOCUMENTS UNDER THE INDIAN EVIDENCE ACT AND IT ACT**

---

### **A. The Section 65B Certification Requirement**

Section 65B of the Indian Evidence Act, which was enacted through the Information Technology Act, 2000, primarily governs the admission of electronic evidence in India. According to this clause, a certificate from a responsible party must be included with any electronic document used as proof. The device used to make the record must be identified in this certificate, which must also attest to the device's regular use, proper operation, and creation of the record during routine activities [8].

The Supreme Court ruled in *Anvar P.V. v. P.K. Basheer* that electronic evidence must adhere to Section 65B in order to be admitted. According to the Court, electronic records are typically not admissible without the necessary certificate [9].

The Supreme Court later clarified that the certificate may be provided at any point prior to the official presentation of the evidence in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*. The Court further clarified that the person in charge of or in possession of the device from which the electronic record was generated is responsible for providing the certificate [10].

### **B. AI-Generated Documents: The Attribution Problem**

AI-generated documents pose new challenges that Section 65B cannot cope with effectively. The generation of documents by any AI technology, whether a language model, a predictive algorithm, or a machine learning software program, implies that the document does not come from an identifiable computer operating in its ordinary course. It comes from a complicated

network of computers, algorithms, data entry, and decisions, which can sometimes span across several countries [11].

The requirement under Section 65B that the issuing person identifies “the computer” where the electronic record has been generated poses some difficulties for modern AI-based operations since they depend on the operation of a network of interrelated servers instead of one particular computer. Furthermore, the phrase “in the ordinary course of business,” which means that a human oversees these activities regularly, can become problematic when dealing with fully automatic AI.

### **C.The Digital Signature Framework in the IT Act and Its Shortcomings**

The framework of digital signatures in the IT Act, which is regulated under Sections 3 and 5, enables the use of asymmetric cryptography to authenticate electronic records through digital signatures. Where an electronic record is authenticated using the signature of an authorized signatory, it will amount to legal authentication of the electronic record [12]. Nevertheless, since AI is not capable of being a signatory in accordance with Indian laws, as the concept of signatory implies the capacity for legal personhood, one may wonder how human verification through digital signatures would be an alternative means of ensuring the validity of electronic records.

## **DPDP ACT 2023 CONFLICTS IN CROSS-BORDER ARBITRATION DOCUMENT PRODUCTION**

---

### **A. The Architecture of Data Localisation and Consent**

The Digital Personal Data Protection Act, 2023 mandates a consent-driven model for the processing of digital personal data along with several prohibitions in respect of cross-border transfer of such data. Under Section 16 of the DPDP Act, the Central Government has been vested with the power to notify jurisdictions to which data may be transferred, thus making it

a white list approach [13]. Any transfer of personal data by data fiduciaries outside the whitelisted jurisdiction requires prior authorization.

In international arbitration proceedings, routine requests for document production necessitate the transfer of massive amounts of documentary information across international borders, which can include confidential information in communications, financial documents, and staff records as well as personal data, as referred to in the DPDP Act. If the seat of the arbitration proceedings is situated in a jurisdiction that has not been notified under Section 16, or where there is a need for disclosure of the documents to foreign counsel, adversaries, or foreign arbitrators, the data fiduciary would face a dilemma.

### **B. Lack of an Arbitration Exception**

Another important shortcoming with the DPDP Act, 2023 is the lack of an exception in respect of processing personal information for legal proceedings like arbitration. Some of the exceptions that have been incorporated within the scope of the DPDP Act, 2023 relate to state activity, scientific and historical research, and security reasons. There are other exceptions such as “legal obligation” and “legitimate interests” that have been provided under the GDPR [14].

This leads to issues arising in arbitrations. According to Section 24 of the Arbitration and Conciliation Act, arbitral tribunals have the right to compel parties to submit their documents. But when such documents contain personal information and are provided to any party or tribunals outside of India, complying with the order might constitute a violation of the DPDP Act.

Another issue is related to the consent provisions included in the DPDP Act. The sixth section provides that consent for data processing should be freely, specifically, precisely, explicitly, and unambiguously granted. In contrast, any general arbitration clause included in a business agreement will hardly serve as sufficient consent for future data transfers between different countries.

Therefore, arbitration agreements would have to be crafted carefully in order to include such provisions that would authorize cross-border transfer of data during arbitral proceedings in the future.

## **Comparison with the IBA Rules on Evidence and GDPR**

---

### **A. The IBA Rules on Evidence: An International Standard**

The IBA Rules on the Taking of Evidence in International Arbitration, revised in 2020, have gained prominence as the international standard for the treatment of evidence in commercial arbitration cases. Under Article 9(3), tribunals can decline or impose limits on the production of evidence when such production could infringe upon the rights and guarantees that include privacy and data protection laws [15]. The rule has gained significance for international cases where there are potential conflicts between the data protection laws, including GDPR, and evidence requests.

Under the IBA Rules, electronically stored information (ESI) is recognised. In Articles 3(3) and 3(12), parties have the discretion to submit documents as searchable electronic documents, and the tribunals have discretion to establish effective mechanisms for the management of digital evidence [16]. While the rules do not explicitly refer to artificial intelligence-generated evidence or smart contracts, they are sufficiently flexible to cover any technology since documents include electronic documents.

One notable aspect of the IBA Rules is the vast discretionary powers granted to arbitral tribunals in respect of evidentiary issues, including those concerning document production, which is more flexible than India's more prescriptive approach to evidence.

### **B. GDPR: Finding the Middle Ground between Privacy and Arbitration**

Article 6(1)(c) of the GDPR allows processing of personal data to meet any legal obligations, whereas Article 6(1)(f) allows processing of personal data if there are legitimate interests at

stake, provided that the rights of data subjects are not violated [17]. EU bodies have constructed Article 6 of the GDPR to cover litigations and arbitrations.

The GDPR offers various options for the cross-border transfer of personal data, which include standard contractual clauses, binding corporate rules, and adequacy decisions [18]. All these instruments ensure the compliance of parties with privacy law while transferring personal data during arbitration.

In contrast, the DPDP Act of India has adopted a more rigid stance by requiring parties to obtain approval from the Central Government before exporting personal data outside the country. Due to the fact that the list of approved countries is yet to be notified by the Indian government, ambiguity exists for the parties engaging in international arbitration.

### **C. AI-Generated Evidence in International Arbitration**

There have been some developments in relation to the issue of AI-generated evidence within international arbitration forums. For example, in 2023, the ICC Commission on Arbitration and ADR said that arbitrators need to critically assess the validity, accuracy, and reproducibility of any AI-generated evidence along with the extent of human involvement in the process [19].

Likewise, the SIAC recommends that the tools of AI which have been used for document reviews and evidentiary analysis be disclosed by the parties to arbitration proceedings. There is no such guidance available yet from any Indian international arbitral forum like the Mumbai Centre for International Arbitration [20].

## **CONCLUSION**

---

The current Indian system of arbitration is being faced with new issues because of the increasing use of smart contracts and AI evidence in cases. The present-day legislation including the Arbitration and Conciliation Act, Indian Evidence Act, Information Technology

Act and the DPDP Act does not account for these innovations, causing difficulties with proving consent, admitting evidence, and transferring information.

In light of the comparison made above between Indian legislation and international norms, including IBA Rules and GDPR, it becomes apparent that other jurisdictions are handling these kinds of disputes in a more liberal manner than India, which might affect India's ability to attract more international disputes.

In order to maintain its competitive advantage, India needs to adopt certain reform measures, which will include explicit recognition of smart contract arbitration agreements, clear guidelines concerning artificial intelligence generated evidence and an exemption from data processing in arbitration cases.

## CITATIONS

---

1. Arbitration and Conciliation Act, 1996, 7(4)(b), No. 26, Acts of Parliament, 1996 (India), amended by Arbitration and Conciliation (Amendment) Act, 2015, No. 3, Acts of Parliament, 2016 (India).
2. Information Technology Act, 2000, 2(1)(t), No. 21, Acts of Parliament, 2000 (India).
3. Kevin D. Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age* 47–52 (Cambridge Univ. Press 2017).
4. *National Insurance Co. Ltd. v. Boghara Polyfab Pvt. Ltd.*, (2009) 1 S.C.C. 267, 21 (India).
5. *Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd.*, (2010) 3 S.C.C. 1, 14 (India).
6. *Soni Dave v. Trans Asian Shipping Servs. Pvt. Ltd.*, 2016 SCC OnLine Bom 1852 (Bom. H.C.) (India).
7. *Forensic India Pvt. Ltd. v. Tek Chand Prashad*, 2021 SCC OnLine Del 3441 (Del. H.C.) (India).

8. Indian Evidence Act, 1872, 65B, inserted by Information Technology Act, 2000,92 (India).
9. *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473, 24 (India).
10. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1, 51 (India).
11. Gary Marcus & Ernest Davis, *Rebooting AI: Building Artificial Intelligence We Can Trust* 142–58 (Pantheon Books 2019).
12. Information Technology Act, 2000, 3–5 (India).
13. Digital Personal Data Protection Act, 2023, 16, No. 22, Acts of Parliament, 2023 (India).
14. Commission Regulation 2016/679, art. 6(1)(c), (f), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
15. Int’l Bar Ass’n, *IBA Rules on the Taking of Evidence in International Arbitration* art. 9(3) (2020).
16. *Id.* arts. 3(3), 3(12).
17. GDPR, supra note 14, art. 6(1)(c), (f).
18. GDPR, supra note 14, arts. 44–49.
19. ICC Comm’n on Arb. & ADR, *Report on Artificial Intelligence and Dispute Resolution* 34–38 (Int’l Chamber of Commerce 2023).
20. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001–7031 (2000).