

ORIGINAL RESEARCH ARTICLE

Digital Sovereignty and the Arbitral Frontier: Resolving Multi-Jurisdictional Technology Disputes through Lex Informatica

Mr Sarthak Sikarwar^{1,*}, Ms Shreya Manoga²

¹ Student, UPES, Dehradun, Uttarakhand

² Student, UPES, Dehradun, Uttarakhand

ARTICLE INFO

Received: 12 September, 2026

Revised: 01 October, 2026

Accepted: 8 October, 2026

Published: 23 October, 2026

KEYWORDS

Lex Informatica; digital sovereignty; international commercial arbitration; delocalization theory; lois de police; UNCITRAL Model Law

ABSTRACT

This paper examines the structural incompatibility between digital sovereignty regimes such as the EU's GDPR, India's DPDP Act (2023) ¹and China's Data Security Law (2021)² and the delocalized, transnational character of international commercial arbitration in technology disputes. It argues that Lex Informatica, understood not merely as technical code but as a coherent normative framework capable of generating enforceable transnational obligations, offers the most jurisprudentially defensible basis for resolving multi-jurisdictional technology disputes in the arbitral forum. Proceeding through doctrinal synthesis and comparative analysis, the paper builds on Reidenberg's conception of Lex Informatica ³and Lessig's 'code is law' thesis⁴, examining how arbitral tribunals may invoke code-based norms under Article 28 of the UNCITRAL Model Law as substantive rules governing the merits of a dispute. It further explores the tension between data sovereignty statutes as mandatory overriding norms (lois de police) and party autonomy, with particular attention to decentralized on-chain arbitration (the Kleros protocol) and Indian law's own readiness for this shift. The paper concludes by proposing a tripartite harmonization framework (the 'Digital Arbitral Sovereignty Compact' (DASC) as a roadmap for reconciling state regulatory prerogatives with the demand for a legally certain, technologically sophisticated dispute resolution architecture.

1. INTRODUCTION: THE CARTOGRAPHY OF A LEGAL CRISIS

1.1 The Geopolitical Rise of Digital Sovereignty

The concept of digital sovereignty – defined as the assertion by nation-states of ultimate regulatory authority over data flows, digital infrastructure and cyberspace within their territorial and jurisdictional borders – has undergone an extraordinary speed and scope of metamorphosis in the opening decades of the twenty-first century. ⁵What was once a marginal academic proposition has become the cornerstone of national security doctrine, trade policy, and legislative architecture across the entire spectrum of geopolitical alignments. With the entry into force of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) in the European Union in 2018, at a supranational level, the paradigm of laissez-faire data economy that had characterized the previous era of digital globalization was definitively

¹ Greenleaf, G. (2024). India's Digital Personal Data Protection Act 2023: A unique addition to global standards. *Computer Law & Security Review*, 52, 105912.

² Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, 8(1), tyac011. <https://doi.org/10.1093/cybsec/tyac011>

³ Reidenberg, J. R. (1997). Lex Informatica: The formulation of information policy rules through technology. *Texas Law Review*, 76(3), 553–593.

⁴ Lessig, L. (1999). *Code: And other laws of cyberspace*. Basic Books.

⁵ Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>

rejected. Combined, the GDPR's extraterritorial reach, its regime of data subject rights, and its draconian sanctions for non-compliance heralded the European regulatory state's willingness to exercise sovereign dominion over personal data regardless of where the processing entity was incorporated or where the data was physically located. China followed with the Data Security Law (2021) and the Personal Information Protection Law (2021), each embodying a nationalist perspective of data governance based on state control over cross-border data flows as an instrument of economic policy and national security. India's passage of the Digital Personal Data Protection Act (2023) reflected many of these structural choices, requiring data localization for sensitive categories, and subjecting offshore data processors to the supervisory jurisdiction of the Data Protection Board of India.

This phenomenon leads to a fragmented normative architecture of global digital regulation which can be referred to as the "Balkanization" of the internet and, as further argued by other scholars, "data nationalism."⁶ Every jurisdiction has established its own compulsory regime regarding data residence, liability, and accountability. Furthermore, they claim that their normative regimes override foreign regulations and even contractual agreements between parties. From the perspective of multinational technology companies, cloud service providers, artificial intelligence developers, and blockchain protocols, it creates an atmosphere of continuous legal uncertainty. If one were to consider an instance in which the AI contract was entered into between a company that operates in Europe, the United States, and India, then GDPR's principle of data minimisation, DPDP's localisation requirement, and CCPA's opt-out provisions might all find themselves competing for priority within the scope of that single question.

1.2 The Failure of Traditional Choice of Law Rules

Private International Law, the field dedicated to the task of determining which national legal system's law should be used in cross-border civil and commercial disputes, was formulated within the context where territorial location was equated with legal personality and jurisdiction. The fundamental principles upon which the field stands, beginning with Friedrich Carl von Savigny's 'seat of the legal relationship' through to the more recent 'most significant relationship' test formulated in Restatement (Second) of Conflict of Laws (1971), operate on the premise that the dispute may be attributed to a specific legal system whose laws would subsequently govern the dispute⁷.

The choice-of-law analysis based on these assumptions breaks down in dealing with disputes created by truly borderless technologies. Let us take, for instance, the legal structure of a dispute arising out of the operation of a smart contract on a distributed blockchain network, which has no place of domicile and runs across nodes in forty-three jurisdictions at any one time, leading to the automated transfer of digital property according to rules of logic written neither by a lawyer nor a judge. Parties can be anonymous, the 'seat' of the agreement is everywhere and nowhere at once, and the code is another normative regime altogether that does not map onto the laws of any nation-state. This exact challenge arose in *Pearson v. Salfi*, though in a more moderate version, and in the continuing discussions of the arbitrability of smart contract disputes in institutional arbitration.

This challenge is further complicated by the practice of forum shopping, which digital business encourages structurally. Digital businesses, for example, regularly use corporate entities in countries with lenient regulations, enter into agreements governed by the law of offshore jurisdictions, and place their technical infrastructure in regions that provide lower latency and energy expenses than those with any normative connection to the parties or the transactions (Mills, 2018). Traditional conflict of laws rules, when applied strictly, often lead to rulings that have little or nothing to do with the regulatory interests of any government and encourage regulatory arbitrage.⁸

⁶ Chander, A., & Le, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677–739

⁷ Symeonides, S. C. (2014). *Codifying choice of law around the world: An international comparative analysis*. Oxford University Press.

⁸ Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press.

1.3 *Lex Informatica as the Arbitral Saving Grace*

In the context of such an apparent doctrinal failure and legal disunity, it is within this framework that the thesis of this paper takes on added significance. The international commercial arbitration system, as a dispute resolution process based on party autonomy, institutional agility, and its lack of localization within any one national legal system, has specific characteristics that make it uniquely suited to handle the intricacies of law created through borderless digital commerce.⁹ Nonetheless, for this purpose, the arbitration system needs a normative basis which can transcend national legal borders without losing its coherence and legitimacy in doing so. In this regard, it is the reconceptualized *Lex Informatica* which fills the bill.¹⁰

The idea of *Lex Informatica* was initially and theoretically proposed by Joel Reidenberg (1998) in a groundbreaking study that proposed that the technical protocols and procedures governing information networks can be considered a form of regulation that is functionally equal to—if not more effective than—the regulations established by legislative bodies and enforced by the judiciary system. Reidenberg noted that information networks have established certain default rules regarding information exchange, defining what actions can and cannot be taken, and imposing normative restrictions without the need for state enforcement for compliance. Lawrence Lessig (1999) later expanded on this idea and coined the now-famous phrase "code is law"—the proposition that software codes regulating computer networks are forms of regulation just as potent and influential as legal regulations, operating mostly beyond the scope of democratic processes.

This Paper posits that the normative content of the *Lex Informatica*, or the technical regulations, standards, protocols, and algorithmic control structures that organize transactions in the digital marketplace, can and ought to be acknowledged by arbitral tribunals as a kind of transnational commercial custom similar to the *Lex Mercatoria* and be applied as the 'rules of law' used in determining the substance of an arbitration under Article 28(1) of the Model Law of UNCITRAL on International Commercial Arbitration.¹¹ By recognizing the applicability of *Lex Informatica*, tribunals will avoid getting bogged down by the unsolvable problems of competing digital sovereignty systems, while at the same time giving the parties concrete legal principles that are well suited to the technical facts of their underlying dispute. The ensuing discussion addresses both the doctrinal objections, the weaknesses of enforcement, and the constitutional challenges inherent in such a view.

2. THE DOCTRINAL CONFLICT: DIGITAL SOVEREIGNTY VS. ARBITRAL DELOCALIZATION

2.1 *The Architecture of Arbitral Delocalisation*

According to the delocalization approach, any arbitral procedure taking place under the terms of an effective arbitration agreement takes place irrespective of the national law regime of the state in which the arbitration is being held. The most extreme form of this theory, espoused by theorists like Jan Paulsson (1981) and Berthold Goldman, states that the effectiveness of the arbitral award lies not in the law of the seat but in the transnational commercial law system; consequently, any award arising out of such arbitral procedure would be binding even if the award had been set aside in the seat (Paulsson, 1981).¹² While this most extreme formulation of the theory has been challenged, for instance by Mann (1983), a moderate version still forms the basis of international commercial arbitration.

⁹ Born, G. B. (2021). *International commercial arbitration* (3rd ed.). Kluwer Law International.

¹⁰ Reidenberg, J. R. (1997). *Lex Informatica: The formulation of information policy rules through technology*. *Texas Law Review*, 76(3), 553–593.

¹¹ Gaillard, E. (2010). *Legal theory of international arbitration*. Martinus Nijhoff Publishers.

¹² Paulsson, J. (1981). *Delocalisation of international commercial arbitration: When and why it matters*. *International and Comparative Law Quarterly*, 30(2), 358–361.

This can be seen, for instance, in the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958), which puts into practice a moderated version of delocalization since it allows the existence of a presumption in Favor of enforcement to be rebutted only for reasons mentioned under Article V, and there is no need for an award to be domesticated within the legal system of the seat prior to being enforceable elsewhere. The UNCITRAL Model Law takes a further step in such a direction through its provisions that allow for parties to agree on using any ‘rules of law’—and not just the law of a national legal system—as the law applying to their dispute (Art. 28(1)) and that authorize arbitrators to function as *amiables compositors* or to rule *ex aequo et bono* provided that the parties have consented in writing (Art. 28(3)).

Indeed, such an architecture is what makes arbitration a promising means of resolving disputes in the field of technology because it allows for the creation of true transnational substantive law that may be derived from general principles of law, from the *Lex Mercatoria*, from standard-setting institutions in particular industries, or, according to this paper, from *Lex Informatica*, without one side having to yield to the legal domination of the other's domestic legal regime.

2.2 Data Sovereignty Statutes as Mandatory Overriding Norms (Lois de Police)

It is the national data sovereignty laws' assertion as mandatory overriding norms, rather than any inherent flaw within the framework of the theory of arbitration, which poses the first danger to the delocalization feature of arbitration in technological disputes. Overriding mandatory provisions are rules of a given legal system that, because of their policy goals and substance, apply regardless of any agreement between the parties regarding which law should apply to the contract relationship (Recital 37, Rome I Regulation (EC) No 593/2008). With regard to the regulation of personal data and governance of technologies, there has been an increasing tendency among lawmakers to clearly state that their legislation is intended to be considered an overriding provision.

Article 3 of the GDPR is a good example. The rules apply to the processing of personal data of data subjects who are in the European Union irrespective of where such processing occurs and irrespective of any agreement between the parties relating to the applicable law. In *Schrems v. Data Protection Commissioner* and the subsequent decision, *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ('Schrems II'), the Court of Justice of the European Union (CJEU) was unequivocal in asserting that GDPR compliance is a non-derogable minimum standard which can never be undermined by private contractual agreements, by foreign law, or even the determination of foreign regulatory authorities—including arbitral awards. The 'Schrems II' ruling found that the EU-US Privacy Shield regime—a regime established by two of the most powerful states in the world in order to ensure cross-border data flows did not provide 'essentially equivalent' data protection standards to those provided by EU law. Such is the significance of this decision for international arbitration: an award ordering a party to conduct a data transfer in contravention of CJEU requirements would be rendered unenforceable in any EU member state on public policy grounds under Article V(2)(b) of the New York Convention.

The DPDP Act of India is faced with a similar structural difficulty. Section 16 of the DPDP Act grants the Central Government the right to notify the countries to which data fiduciaries are permitted to transfer personal data, and this amounts to a whitelist approach whereby the crossing of data by the private parties is dependent on the administrative authority vested in the executive branch, thus making the legality of the data transfer contingent on the decision of the executive body which can withdraw its decision at will. If an arbitral tribunal were to apply *Lex Informatica* or international commercial law in settling a dispute involving data processing and arrive at the conclusion that the data transfer was permissible, this would be contrary to the administrative determination made by the Data Protection Board of India, in which case the defeated party could object to the arbitral award being enforced under Section 44 of the DPDP Act.

Yet again, DSL and PIPL give rise to serious structural contradictions. According to Article 31 of the DSL, the 'important data' created or collected in China should be processed and stored on Chinese territory, and any attempt at transferring data abroad is subject to a security assessment by the authorities. The scope of 'important data' under implementing guidelines is quite extensive, and the process of conducting security assessments remains unclear and can take indefinitely long. In such circumstances, an international technology corporation whose disputes in Singapore are governed by the SIAC Rules (as well as English law) and who is awarded a remedy for its claims, can face the situation whereby the data elements of that judgment become impossible to enforce against the counterparty based in China due to a violation of DSL, a matter that constitutes a criminal offense under Chinese law and which is viewed as contrary to public policy there.

2.3 Kompetenz-Kompetenz and the Limits of Arbitral Jurisdiction over Mandatory Rules

The Kompetenz-Kompetenz principle, which gives the arbitral tribunal competence to make determinations about its jurisdiction, including whether an arbitration agreement exists or is valid, is one of the core principles of contemporary arbitration law, enshrined in Article 16 of the UNCITRAL Model Law and found in almost all institutional arbitration rules, including in ICC Arbitration Rules 2021 (Article 6) and SIAC Arbitration Rules 2025 (Article 29). This principle gives arbitral tribunals the procedural ability to decide, at least initially, whether any given dispute is within their jurisdictional mandate.¹³ The Kompetenz-Kompetenz doctrine does not answer the question of whether the tribunal has the ability to ignore mandatory laws that a sovereign state has made non-derogable.

The interaction between mandatory rules and the jurisdiction of the arbitration process was considered by the English Court of Appeal in *Soleimany v. Soleimany* [1999] QB 785 when it denied recognition of an arbitral decision as its enforcement would require actions that would be unlawful in terms of the foreign country's law and, also, by the Swiss Federal Tribunal through a set of decisions which have established the rule that the enforcement of an arbitral award cannot be based on the requirement of performing any action that is clearly opposed to the fundamental policy of the forum state. Most recently, in *Dallah Real Estate and Tourism Holding Company v. Ministry of Religious Affairs of the Government of Pakistan* [2010] UKSC 46, the Supreme Court of the United Kingdom recognized the fact that jurisdiction issues involving mandatory rules of public law fall within the ambit of de novo judicial review.

The implication in terms of technology arbitration is that any arbitral panel that endeavours to rule on such technological disputes based solely on Lex Informatica or transnational law without taking into account the mandatory provisions of the relevant data sovereignty legislation binding upon one or both of the disputants runs the risk of rendering an award that would not be enforceable in the very jurisdictions where enforceability is economically crucial. The critical doctrinal dilemma underlying the rest of this paper is this: Can Lex Informatica be implemented through arbitration in a way that preserves its nature as an exercise of delocalization of international arbitration while guaranteeing enforceability of the award despite the conflicting mandatory principles of digital sovereignty?¹⁴

3. DECONSTRUCTING LEX INFORMATICA IN THE ARBITRAL FORUM

3.1 Code as Self Executing Substantive Law

The basic premise of the research by Reidenberg (1998) was the realization that technology architecture not only aids in legal compliance but is also itself a system of regulations, which works more efficiently than laws passed by governments. This idea gains a special legal significance when applied to smart contracts, which are programs running in blockchain networks that automatically execute the provisions of an agreement based on certain specified events. Smart contracts are much more than just a

¹³ Born, G. B. (2021). *International commercial arbitration* (3rd ed.). Kluwer Law International.

¹⁴ ICCA-IBA Joint Task Force on Data Protection in International Arbitration. (2022). *The ICCA-IBA roadmap to data protection in international arbitration* (ICCA Reports No. 7). International Council for Commercial Arbitration.

representation of legal agreements; from a philosophical point of view, smart contracts constitute legal agreements themselves, which operate through coding and execution of these codes by computers. Once certain conditions are met, there is no need for any human intervention because smart contracts automatically fulfill their functions, without the necessity of enforcement or even agreement from the parties involved in their execution.

The jurisprudential implications of the self-executing nature of the smart contract have been explored by few, if any, legal scholars prior to Werbach and Cornell's 2017 analysis. According to Werbach and Cornell, the so-called 'oracle problem', which refers to the difficulty of relating smart contracts to off-chain legal conditions (i.e., the existence of an existing legal dispute, the acquisition of a particular legal status, or a fulfillment of a contractual condition contingent upon non-blockchain facts) is the main technical and legal issue associated with the use of smart contracts in business dealings. The 'oracle problem' is both technical and jurisprudential at the same time. In light of their view that code is law within the confines of smart contract transactions, the 'interpretation' of such contract code should involve neither hermeneutic interpretation nor any other form of legal interpretation, but rather a technical one.

From the perspective of arbitral tribunals, this is an analytical problem that manifests itself as a form of jurisdictional and evidentiary problem. First, the tribunal set up to adjudicate in the dispute stemming from a smart contract must be technically competent enough to evaluate the expert evidence pertaining to the functioning of the code in question; second, it should be able to determine the nature of the legal gap, if there indeed exists one, between the functioning of the code and the intent of the parties under the contract; finally, it should have a substantive normative framework capable of addressing this legal gap in a coherent fashion. *Lex Informatica*, defined as a set of technical standards and governance norms relevant to the blockchain or digital platform in question, is the best framework for doing just this.

3.2 Algorithmic Governance as an Extension of the Lex Mercatoria

The analogy of *Lex Informatica* to the *Lex Mercatoria*, which was the collection of business practices, customs, and generally accepted norms for the conduct of transactions across national borders by medieval merchants that has been revived in the contemporary context as a possible foundation for transnational business law, is a useful comparison both legally and juristically. The *Lex Mercatoria* gained recognition as a source of law relevant to international business arbitration as a result of the writings of Goldman (1964) and Schmitthoff (1961) and, more recently, the UNIDROIT Principles of International Commercial Contracts (2016), which have been used by arbitrators as the *Lex Mercatoria* in resolving business conflicts (Osman, 1992).¹⁵

The basic argument for the *Lex Mercatoria* being an acceptable source of arbitral law is founded upon three pillars: (i) that businessmen within a particular industry have developed mutual understandings, traditions, and ways of doing business which represent a truly normative framework; (ii) that such norms are sufficiently clear and consistent enough to be articulated; and (iii) that their enforcement through arbitral tribunals leads to results which are much more in tune with the justified expectations of the parties involved than the rigid enforcement of a national law regime selected according to the criteria of conflicts of law.¹⁶ The same argument may be made in Favor of *Lex Informatica* in disputes involving technology. The technical standards and protocols regulating the digital technology industry, including the Internet Engineering Task Force (IETF) Request for Comments (RFC) standards, the Web standards of the W3C, the IEEE standards for e-commerce transactions, and the protocol standards and documentation regulating the behaviour of large blockchain networks like the Ethereum Improvement Proposals (EIPs) of Ethereum and Bitcoin Improvement Proposals (BIPs) of Bitcoin, is a set of normative standards that satisfy all three of Goldman's criteria for *Lex Mercatoria*. There is common agreement between technology actors on what

¹⁵ Berger, K. P. (2010). *The creeping codification of the new lex mercatoria*. Wolters Kluwer.

¹⁶ Gaillard, E. (2010). *Legal theory of international arbitration*. Martinus Nijhoff Publishers.

these standards mean; they have been developed to a level of detail far beyond that of the customary practice of the medieval merchant; and finally, they provide substantive guidance for solving disputes involving disputes about the behaviour and liability created by technological systems, which is something that cannot be replicated by any national legal system. In the arbitration of disputes concerning the malfunctioning of a smart contract due to the re-entrancy vulnerability in Ethereum—the same sort of vulnerability which led to the now infamous DAO hack in 2016—a tribunal can arrive at a more principled judgment and one that is more consistent with the actual technology, by applying standards from the EIPs.

3.3 Legal Points and Key Conflicts in Indian Law

Within the Indian legal ecosystem specifically, the tension mapped in the preceding sections crystallises around four recurring points of legal conflict: the friction between contractual party autonomy and statutory overriding norms; the unsettled arbitrability of intellectual property and patent disputes; the collision between data localization mandates and the free cross-border flow of information; and the unresolved status of artificial intelligence tools used within the arbitral process itself. Each of these fault lines tests whether the Indian legal order can accommodate Lex Informatica as a valid source of substantive law under Article 28 of the UNCITRAL Model Law, as adopted domestically through Section 28 of the Arbitration and Conciliation Act, 1996. The 2026 Québec decision in *ARIHQ v. Santé Québec*, discussed in the due process analysis below, illustrates precisely this last fault line materialising in practice. Whether the existing statutory architecture is equal to this task depends on which layer of the framework is examined. In certain respects, Indian law provides a solid foundation: the general arbitration framework under Sections 34 and 37 of the Arbitration and Conciliation Act, 1996, read with the Supreme Court's consistently pro-arbitration jurisprudence, supplies a reasonably predictable base for enforcement and minimal curial intervention; equally, sectoral data localization rules issued by the Reserve Bank of India, the Telecom Regulatory Authority of India and the Securities and Exchange Board of India offer clear, if narrow, guidance in the financial, telecom and securities sectors respectively.

In other respects, however, the framework remains markedly insufficient. The arbitrability of intellectual property and patent disputes continues to rest on an unsettled body of case law rather than clear legislative guidance, leaving tribunals to improvise on a question central to most technology disputes. The Digital Personal Data Protection Act, 2023 compounds this uncertainty: its cross-border transfer regime under Section 16 vests the Central Government with broad, largely unreviewable discretion, unaccompanied by the legislative safeguards ordinarily attached to such executive power. The Act is equally silent on the growing use of artificial intelligence tools within adjudicatory processes, leaving Indian law blind to what might be termed the 'fourth party' now routinely present at the arbitral table. Finally, Section 7(c) of the DPDP Act permits non-consensual processing of personal data on loosely defined 'security of the State' grounds, without any independent oversight mechanism — a surveillance-enabling gap that sits uneasily beside the due-process guarantees arbitral tribunals are expected to uphold. Taken together, these gaps suggest that Indian law, while broadly hospitable to arbitration as a mechanism, has yet to develop the specific doctrinal tools required to accommodate Lex Informatica-based technology disputes with full legal certainty.

3.4 Article 28 of the UNCITRAL Model Law as the Arbitral Gateway

The doctrinal gateway for the entrance of Lex Informatica into the arbitral forum as the applicable substantive law is Article 28 of the UNCITRAL Model Law. The UNCITRAL Model Law Article 28(1) states that the arbitral tribunal should render its award on the merits of the dispute 'in accordance with such rules of law as are chosen by the parties as applicable to the substance of the dispute.' It was the deliberate choice of the drafters to employ the expression 'rules of law' instead of 'the law of a State' in order to allow transnational rules of law, general principles of law, and other non-national legal norms to

be used as the substantive law of the contract (UNCITRAL Secretariat Commentary, 1985). Subsequent interpretation has consistently upheld the drafting intention: the Tribunal in ICC Case No. 6527 (1991) determined that the parties were entitled to choose the 'general principles of international commercial law' as the applicable law; the SIAC Tribunal in multiple awards has relied upon the UNIDROIT Principles as the substantive law under Article 28-equivalent clauses in the SIAC Rules.

The key analytical step necessary to give operation to Lex Informatica through Article 28 entails the ability to show that the rules and protocols that govern a particular information technology network can be characterized as 'rules of law' in accordance with Article 28, such that they are rules that have a degree of normative clarity, consistency, and recognition in the concerned business world that enables their use as an objective standard against which the actions of the parties can be judged.¹⁷ Such an analytic endeavour is more than just a theory; it involves a comparative legal analysis of the rules themselves.

A number of considerations point towards an affirmative answer. To begin with, the systems for governance within leading technical standard-setting organizations, such as the IETF's RFC process, IEEE's balloting, and Ethereum Foundation's EIP review system, incorporate deliberative processes of legitimacy, which are not substantially different from, and in many ways even more transparent than, the process involved in the creation of national legal rules. Secondly, the use of technical standards to resolve disputes does not entail any legislative discretion but rather involves the task of interpretation of an existing set of normative guidelines by experts, a task routinely performed by arbitral tribunals while interpreting complex financial regulations, industry codes of conduct, or professional standards. Finally, and perhaps most importantly, the parties to a technology-related contract would have negotiated the terms of their relationship on the premise that technical standards governing the platform would guide their behaviour; hence, using these standards as the governing law of the dispute represents the approach best aligned with the parties' reasonable expectations - the guiding principle of contract law.¹⁸

4. PROCEDURAL FRONTIERS AND ENFORCEMENT VULNERABILITIES

4.1 The On-Chain Arbitration Frontier: Kleros and Decentralized Justice

The implementation of on-chain decentralized dispute resolution protocols is the ultimate form of the Lex Informatica concept manifested through procedure. In 2018, the platform Kleros was introduced, which operates as a decentralized autonomous organization on the Ethereum blockchain. It offers an automated dispute resolution process where randomly selected 'jurors' who stake cryptocurrencies resolve the disputes by voting on the outcome using tokens, resulting in an automated execution of decisions through smart contracts. Over tens of thousands of disputes that have been decided upon by the Proof of Humanity and the General Court procedures of the Kleros protocol, many e-commerce disputes, token disputes, and smart contract disputes were resolved.

On the level of jurisprudence, Kleros, as well as similar protocols like Aragon Court (now rebranded as Aragon Dispute Resolution), and the JAMS Metaverse Arbitration scheme, pose a formidable jurisprudential challenge to the conventional conception of arbitration as a form of consensus-based dispute resolution, supervised by institutions, and regulated procedurally. For starters, the Kleros protocol lacks certain characteristics of arbitrability that have been conventionally deemed necessary for the legality and acceptance of an arbitral award. These include the absence of a requirement for the juror to be qualified legally; a randomly selected staking pool, not merit-based, for selecting the jury; an unclear deliberation process without any rationale given for a decision; and automatic smart-contract execution as the means of enforcement that does away completely with court supervision under the New York Convention.

¹⁷ Moses, M. L. (2019). *The principles and practice of international commercial arbitration* (3rd ed.). Cambridge University Press.

¹⁸ Bermann, G. A. (2017). "International standards" as a choice of law option in international commercial arbitration. *American Review of International Arbitration*, 27(4), 423.

The advocates of the Kleros-type decentralized arbitration scheme contend that these perceived flaws are actually virtues: the random drawing of jurors precludes corruption and forum shopping; the token staking process induces a financial motive to reach truthful decisions (Schelling point method); and the automation of the award execution process circumvents the problem of enforcement, which renders arbitral awards irrelevant from a business standpoint when dealing with uncooperative opponents with no property within jurisdictions having an effective judicial system. There is certainly some practical logic behind this reasoning in regard to the particular situation of disputes involving small amounts of money and technologically uniform issues (e.g., e-commerce refunds or NFTs).

Nevertheless, the constraints of decentralised on-chain arbitration are evident when considering disputes that involve high-stakes and complicated technology-related issues. The dispute between parties regarding the cross-border provision of AI services and their GDPR compliance, a disagreement over intellectual property licensing for blockchain content distribution platforms, and cloud computing service disputes concerning conflicting claims over data sovereignty in the EU, India, and China, among other examples, cannot be resolved through the deployment of a set of simple facts by non-specialized jurors. No existing on-chain arbitration system is capable of delivering the necessary legal expertise, and the structural constraints of decentralized decision-making processes, in particular, the lack of deliberation, reasoning, and appeals—are inherently incapable of addressing disputes that have important public policy implications.

4.2 Institutional Tech Arbitration: SVAMC, SIAC, and ICC Frameworks

While on-chain dispute resolution is yet to mature, the institutional infrastructure for resolving technology disputes has made considerable progress in recent years. The Silicon Valley Arbitration & Mediation Centre (SVAMC) founded in 2017, was the first organization to create a set of special arbitration rules tailored specifically for resolving technology disputes, such as provision for a technically qualified tribunal, an accelerated process for emergency cases of intellectual property, and a special procedure for evaluating the evidence regarding the source code and algorithms. The SVAMC Technology Arbitration Rules (as amended in 2023) have made a notable contribution to the creation of Lex Informatica within the arbitral community – recognizing that 'the applicable rules of law' could include technical standards and industry protocols, and also providing special procedures for selecting technical assessors who would help the panel evaluate evidence on how digital systems behave.

SIAC has created a separate innovation track through its SIAC-SIMC Arb-Med-Arb Protocol and its recent Practice Notes for the arbitration of technology disputes (2024). Singapore's aspiration to be the international centre for dispute resolution within the digital economy, as seen in its Singapore Convention on Mediation (2019) and Model Artificial Intelligence Governance Framework by Infocomm Media Development Authority, creates a positive institutional context for the evolution of arbitral doctrine on Lex Informatica issues.¹⁹ The open-ended provision of Rule 31(1) of SIAC Rules regarding 'rules of law' along with its efficient and reliable judiciary system for the recognition and enforcement of arbitral awards makes SIAC an ideal forum for Lex Informatica arbitrations.

In relation to technology disputes at the forefront of the field, the International Chamber of Commerce (ICC) has taken steps in the form of its Digital Economy Taskforce reports (2019, 2022), as well as its creation of tailored arbitration clauses for blockchain and AI-based contracts within its Model Contracts series. The ICC's financial services and fintech disputes department has successfully resolved a range of smart contract and cryptocurrency-based disputes in recent years, establishing an emerging practice in

¹⁹ United Nations. (2018). United Nations Convention on International Settlement Agreements Resulting from Mediation (Singapore Convention on Mediation) (opened for signature at Singapore 7 August 2019; entered into force 12 September 2020). See also Infocomm Media Development Authority & Personal Data Protection Commission. (2020). Model artificial intelligence governance framework (2nd ed.). Singapore: IMDA/PDPC

relation to the admissibility of blockchain-based evidence as well as the legal standards relating to algorithmic decision-making.²⁰ Due to its financial weight and standing as an arbitration organization as well as the fact that ICC awards have binding force internationally thanks to the recognition accorded to them by courts worldwide, it is in an ideal position to establish precedents in Lex Informatica.

4.3 The Enforcement Crisis: Article V and the Public Policy Gateway

The critical weakness in enforcement through technology arbitration is the public policy exception contained in Article V(2)(b) of the New York Convention, which allows enforcing courts to deny recognition to arbitral awards if recognition would run counter to the public policy of the state where recognition is sought. The travaux préparatoires of the New York Convention suggest that the public policy exception was designed to be interpreted restrictively, representing a backstop against arbitral awards which violate the bedrock foundations of legality and morality in the enforcement jurisdiction. Yet the meaning of 'public policy' in the domain of digital governance continues to expand as data sovereignty statutes define data protection principles in terms of fundamental rights and national security – factors which necessarily hold some bearing under the rubric of Article V(2)(b).

Whether data sovereignty legislation may be classified as "public policy" in accordance with Article V(2)(b) is an unresolved question in the doctrinal context at this point in time. Nevertheless, based on the recent development in jurisprudence following the enactment of the GDPR, there exists considerable danger in the expanded interpretation of public policy under Article V(2)(b). In terms of the case law on the matter of EU competition law, the CJEU ruling in *Eco Swiss China Time Ltd v. Benetton International NV* (Case C-126/97, 1999) affirmed that fundamental laws of the EU amount to public policy pursuant to Article V(2)(b) and further extended this concept to make intra-EU investment arbitration subject to EU public policy in *Achmea BV v. Slovak Republic* (Case C-284/16, 2018) in which some types of arbitral awards were found to be unenforceable within the EU territory due to public policy considerations.²¹ The likelihood of applying this principle to GDPR is therefore highly probable.

The impact of a wide conception of public policy upon the binding nature of a Lex Informatica award is severe. Where a dispute regarding data rights has been arbitrated by a tribunal under the substantive provisions of the blockchain protocol, allowing for the movement of data in contravention of Chapter V of the GDPR where no measures are provided, a claim pursuant to Article V(2)(b) could arise against such award in any enforcement court in the EU.²² This is equally true where DSL rules of China or DPDP Act rules of India are applicable. In short, a perfectly good award from a jurisprudential standpoint is potentially of no commercial value insofar as it could not be enforced because of the operation of public policy in the enforcement jurisdiction.

4.4 Due Process Challenges in Algorithmic Awards

There is a different enforcement risk, albeit similar in nature, posed by the due process obligations stipulated under Article V(1)(b) of the New York Convention, which allows enforcement to be denied when the party who is against whom the award is claimed cannot state their case. In the case of algorithmic arbitration, whether it is fully decentralized, as seen in the Kleros project, or even partial automation, as seen in the fast-track processes in technology arbitrations, there is an actual chance that the pace and efficiency of the procedure could prevent the parties from challenging the technical data behind the award,

²⁰ ICC Commission on Arbitration and ADR. (2022). Leveraging technology for fair, effective and efficient international arbitration proceedings (ICC Commission Report). International Chamber of Commerce.

²¹ Bermann, G. A. (2012). Navigating EU law and the law of international arbitration. *Arbitration International*, 28(3), 397.

²² ICCA-IBA Joint Task Force on Data Protection in International Arbitration. (2022). The ICCA-IBA roadmap to data protection in international arbitration (ICCA Reports No. 7). International Council for Commercial Arbitration.

cross-examining experts regarding the workings of the algorithm, and providing alternative perspectives to the code itself, which forms the substance of the law governing the dispute.²³

However, the problem is especially relevant to AI-supported arbitral proceedings since some arbitral institutions, like the ICC and SIAC, consider implementing such an idea as an effective method to deal with increasingly complex cases concerning digital economy disputes. If the AI tool supports the tribunal in its deliberations in terms of decoding algorithms and analyzing their performance or applying specific standards, and at the same time, the parties lack access to the very process of reasoning of the AI tool because it is, for example, a so-called black box due to the peculiarities of the large language model reasoning used in the AI software, then there is strong ground to believe that such an award fails to meet the due process standards set out in the New York Convention or in the principles of natural justice applied by national courts to arbitral decisions.²⁴

This risk is no longer speculative. In *ARIHQ v. Santé Québec* (2026 QCCS 1360), decided on 22 April 2026, the Québec Superior Court set aside an arbitral award upon finding that the arbitrator had relied exclusively on AI-generated hallucinated authorities — including fictitious case law and academic sources — which formed the core of the reasoning, thereby violating principles of party autonomy, reasoned decision-making, and deliberative confidentiality. The ruling is the clearest judicial confirmation to date that the black-box risk identified above is not merely theoretical: where an AI tool's undisclosed reasoning process supplies the substantive content of an award rather than merely assisting the tribunal, reviewing courts will treat the resulting award as void for want of a genuine, reasoned decision by the arbitrator. *ARIHQ* accordingly reinforces the case for the disclosure and verification safeguards proposed in this paper's concluding roadmap, and confirms that Lex Informatica's promise as a substantive source of law must be kept analytically distinct from the separate, and considerably more dangerous, practice of allowing AI systems to silently author the reasoning of an award itself.

These issues of enforcement are not critical to the idea of lex informatica arbitral proceedings, but they do represent important constraints that have to be considered in the design of such an institution. The final section of this paper will outline a strategic path that takes into account each of these issues, while still adhering to the central idea that of lex informatica in an international commercial arbitral process being the best mechanism for dispute resolution in today's regulatory environment.

5. CONCLUSION & STRATEGIC ROADMAP: THE DIGITAL ARBITRAL SOVEREIGNTY COMPACT

This paper has shown that the problem of digital sovereignty versus arbitral delocalization cannot be seen as some sort of legal esoterica or mere academic exercise but, rather, stands at the heart of the fundamental questions confronting modern international commercial arbitration in the era of digitization. The emergence of mandatory digital sovereignty legislation – such as the GDPR, the DPDP Act, and the DSL/PIPL – has produced an environment in which conflict of laws rules simply no longer apply to the settlement of cross-border technology disputes, and in which arbitral awards are endangered due to an expansion of public policy defences based on the conception of data governance as a constitutional and national security issue. This paper has contended that Lex Informatica, understood as the product of technical standards, protocol governance, and algorithmic architecture, provides the soundest substantive law basis for technology arbitration under the auspices of the Model Law's Article 28, and consistent with the delocalization concept enshrined within the New York Convention.²⁵

²³ Cosío Patiño, G. (2022). Lex cryptographia guidelines for ensuring due process in transnational blockchain-based arbitration: Study on the Kleros model. *Transnational Dispute Management*, 5; Bergolla, L., Seif, K., & Eken, C. (2022). Kleros: A socio-legal case study of decentralized justice & blockchain arbitration. *Ohio State Journal on Dispute Resolution*, 37(1), 55–98

²⁴ Scherer, M. (2019). Artificial intelligence and legal reasoning: To what extent can AI tools support or replace arbitral tribunals? *Journal of International Arbitration*, 36(5), 539–550.

²⁵ Mustill, M. J. (1988). The new lex mercatoria: The first twenty-five years. *Arbitration International*, 4, 86.

In order to operationalize this jurisprudential argument, this paper introduces the idea of the 'Digital Arbitral Sovereignty Compact' (DASC)—a multilayered harmonization scheme built at the nexus of treaties, institutions, and standards regimes.

Firstly, the core element of the DASC is a multilateral instrument on dispute resolution in technology, patterned structurally after the BEPS Multilateral Instrument used in tax treaties.²⁶ Such an instrument will obligate parties thereto to: (i) view algorithmic governance standards and technical protocol documentation as 'rules of law' under Article 28(1) of the UNCITRAL Model Law; (ii) adopt a limited construction of 'public policy' issues in technology arbitration enforcement cases, which requires demonstrating the existence of a particular, real incompatibility with a constitutional right or a national security interest in technology arbitration enforcement, but not with any generic data sovereignty statute; and (iii) create specialized national Technology Arbitration Enforcement Panels of judicial experts who shall resolve Article V problems in technology arbitration enforcement cases within ninety days.

A second pillar, an Institutional Protocol for Lex Informatica Arbitration (IP-LIA), should be collaboratively drafted and promulgated by SIAC, SVAMC, ICC, and UNCITRAL as an additional protocol for use with their respective arbitration rules. Such a protocol would set forth: mandatory minimum qualifications for arbitrators adjudicating technology-based claims, including technical literacy relative to the underlying platforms or protocols in dispute; a standing panel of Technical Standards Assessors—experts in technology certification, qualified and appointed by recognized standards institutions—as resources available to all 25 Mustill, M. J. (1988). *The new lex mercatoria: The first twenty-five years*. *Arbitration International*, 4, 86. 26 Organisation for Economic Co-operation and Development. (2014). *Developing a multilateral instrument to modify bilateral tax treaties, Action 15: 2014 deliverable*. OECD Publishing. See also OECD. (2016). *Multilateral convention to implement tax treaty related measures to prevent base erosion and profit shifting* (text finalised 24 November 2016). Tribunals hearing Lex Informatica cases; protocols for the introduction and interpretation of technical standards in arbitral proceedings, as evidence of applicable law; and a transparency protocol regarding the application of AI analytical tools by arbitral tribunals, with access to and sufficient opportunity provided for challenging such applications afforded to parties.

A third pillar is a Technical Standards Legitimacy Framework (TSLF), created under the aegis of UNCITRAL and the International Organization for Standardization (ISO). The TSLF will establish criteria for identifying and cataloguing those standards and protocol documentation that are considered to be 'Lex Informatica', criteria focusing on deliberative legitimacy, documentary precision, community acceptance and interpretive consistency, and will create a public repository for those standards recognized by arbitral tribunals.²⁷

The philosophical implications of this research go far beyond practical issues of dispute settlement. Is it possible for artificial intelligence-driven by humans—to function as a source of law; is it possible for code to become law, in any legally meaningful sense, of the commercial relations between people? The paper answers this fundamental question affirmatively, while recognizing that it has to be supplemented with a series of institutional reforms that will ensure that all legal principles of procedural justice, legitimacy, and democracy are observed and upheld.²⁸ The creation of the Digital Arbitral Sovereignty Compact is seen as a crucial first step towards a truly transnational legal system of the digital economy, where the code of commercial relations and the law used to settle disputes over them are finally recognized as parts of one and the same legal undertaking.

²⁶ Organisation for Economic Co-operation and Development. (2014). *Developing a multilateral instrument to modify bilateral tax treaties, Action 15: 2014 deliverable*. OECD Publishing. See also OECD. (2016). *Multilateral convention to implement tax treaty related measures to prevent base erosion and profit shifting* (text finalised 24 November 2016).

²⁷ De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The new lex informatica. *Frontiers in Blockchain*, 3, 1–14. <https://doi.org/10.3389/fbloc.2020.00028>

²⁸ Brownsword, R. (2020). *Law, technology and society: Re-imagining the regulatory environment*. Routledge.