

RESEARCH ARTICLE

Doctrinal & Comparative Legal Research

Governance of Artificial Intelligence in Institutional Arbitration

*Towards a Legal Framework for Confidentiality Protection
and Data Security*

Dr. Ali Saleh Ali Al-Fakir

International Legal Expert in International Law and Arbitration
International Attorney · Member, International Court of Arbitration
Member, International Bar Association (IBA)
Vice President for International Relations, Princonser University

FIELD	Private International Law · International Commercial Arbitration · Technology Law
JOURNAL	International Journal of Law and Strategic Studies (IJLSS)
VOLUME	Volume 1, Issue 1 (2026)
PUBLISHER	Hague Solutions and Consultancy

ABSTRACT

This research addresses a legal question of pressing contemporary relevance against the backdrop of the accelerating integration of generative artificial intelligence tools within international institutional arbitration proceedings: namely, the challenge of reconciling the efficiency of such technologies with the preservation of confidentiality as a foundational pillar without which arbitration cannot function. The study subjects the existing international legal framework—both legislative and institutional—to critical examination, revealing a structural deficiency manifested in the absence of binding and consistent provisions governing this integration.

The research contributes two theoretical and practical proposals: first, the concept of ‘Confidentiality by Design’, drawn by analogy from the principle of ‘Privacy by Design’ enshrined in the EU General Data Protection Regulation (GDPR); and second, a model contractual framework governing the use of artificial intelligence tools in arbitration agreements. The study adopts a doctrinal and comparative methodology, with detailed analysis of the rules of the International Chamber of Commerce (ICC), the London Court of International Arbitration (LCIA), the Stockholm Chamber of Commerce (SCC), the EU AI Act, and the SVAMC and AAA-ICDR principles.

KEYWORDS

Confidentiality in Arbitration · Generative Artificial Intelligence · ICC, LCIA, SCC Rules · EU AI Act · SVAMC Principles · Confidentiality by Design

TABLE OF CONTENTS

Introduction: Context, Research Problem, and Research Questions

Part One — Theoretical Framework: Confidentiality and AI in International Commercial Arbitration

1.1 The Concept and Scope of Confidentiality in International Commercial Arbitration

1.2 Generative AI and Its Applications in Arbitration

1.3 Structural Tensions between the Nature of AI and the Principle of Confidentiality

Part Two — The International Legal and Institutional Framework: A Critical Assessment

2.1 The UNCITRAL Model Law and National Legislative Frameworks

2.2 The EU AI Act and the UK AI White Paper

2.3 Institutional Arbitration Rules — A Comparative Study

2.4 Specialized Guidelines — SVAMC and AAA-ICDR

Part Three — Towards a Comprehensive Legal Framework for Confidentiality Protection

3.1 Contractual Provisions and Procedural Confidentiality Orders

3.2 Proposed Model Clauses for AI-Assisted Arbitration

3.3 ‘Confidentiality by Design’ — Theoretical Basis and Practical Application

Conclusion: Findings and Recommendations

References

INTRODUCTION

I. General Context and Significance of the Subject

International commercial arbitration has undergone a profound structural transformation since the early years of the third decade of the twenty-first century, with generative artificial intelligence tools penetrating its successive stages at an accelerating pace: from arbitrator selection and document management, through evidence analysis and the review of arbitral and judicial precedents, to assisting arbitral tribunals in drafting the reasoning of their awards. The 2023 Bryan Cave Leighton Paisner (BCLP) Report indicates that two-thirds of legal professionals support the regulation of AI in international arbitration, reflecting broad awareness of the risks accompanying this technology.

Confidentiality in international commercial arbitration is not merely a procedural virtue; it is the fundamental objective that renders arbitration the preferred alternative to national courts for many multinational corporations and international investors, guaranteeing that the parties' commercial secrets and sensitive information are shielded from public exposure and competitors. Yet the use of AI tools owned by third-party companies—such as ChatGPT and OpenAI systems—results in the deposit of this confidential information in platforms of a collective and shared character, constituting a direct threat to the principle of confidentiality that existing institutional rules have yet to adequately address.

II. Research Problem

The research problem emerges from a structural contradiction between two conflicting requirements: artificial intelligence demands continuous feeding with vast datasets to enhance the accuracy of its outputs, while confidentiality requires that information relating to the dispute remain within a closed ambit inaccessible to third parties. The complexity is compounded by the fact that the current legal framework—both legislative and institutional—lacks binding and comprehensive provisions to adequately govern this integration.

Accordingly, the research problem is organized around a central question: *How can a comprehensive legal framework be constructed to permit the deployment of artificial intelligence in institutional arbitration while preserving the principle of confidentiality and ensuring data security?* Two subsidiary questions derive from this central inquiry: first, to what extent does the existing international legal framework suffice to address the challenges posed by AI to confidentiality in arbitration? And second, what legal, contractual, and technical mechanisms can achieve a balance between AI efficiency and the safeguarding of confidentiality?

III. Research Methodology and Structure

This research adopts doctrinal and comparative legal research methodology, a method grounded in the analytical induction of binding legal texts—conventions, rules, and decisions—and their comparison across different systems to identify points of convergence and divergence and to advance proposals for reform. The research structure is organized into three principal parts: Part One addresses the theoretical framework; Part Two critically analyses the existing legal framework; and Part Three presents proposals and mechanisms to overcome the identified deficiencies.

PART ONE: THEORETICAL FRAMEWORK — CONFIDENTIALITY AND ARTIFICIAL INTELLIGENCE IN INTERNATIONAL COMMERCIAL

ARBITRATION

Section 1.1 — The Concept and Scope of Confidentiality in International Commercial Arbitration

I. Definition and Legal Basis

Confidentiality in international commercial arbitration is a legal obligation binding on the parties, the arbitrators, and all participants in the proceedings to refrain from disclosing any information relating to the dispute or the course of its adjudication to third parties or the public. American jurisprudence has clarified this concept by affirming that ‘confidentiality is a natural outgrowth of the fact that arbitration is a private substitute for state-sanctioned proceedings... and if private arbitration proceedings—held before arbitrators in private locations—had historically been subject to public access, that would have been surprising’.

Confidentiality yields a range of procedural and substantive benefits: it creates a conducive environment for resolving disputes removed from the pressures of media controversy; it prevents the exposure of commercially sensitive information to competitors; it facilitates amicable settlement by reducing the intensity of public posturing; and it establishes a firm system of mutual trust between the disputing parties.

II. Scope and Limits of the Confidentiality Obligation

The confidentiality obligation in arbitration derives from three sources: first, the agreement of the parties, who may expressly stipulate confidentiality in the contract or arbitration agreement; second, the chosen procedural rules and whatever express or implied confidentiality provisions they contain; and third, the law of the seat of arbitration and the extent to which it embraces the principle of confidentiality. Where all three sources are silent on confidentiality, the default position under international arbitral doctrine is that no obligation arises.

It should be noted that the content of the confidentiality obligation is not absolute and admits of exceptions in certain circumstances, most notably: where disclosure is required by a legal duty or is necessary to protect a right or to seek judicial relief.

Section 1.2 — Generative Artificial Intelligence and Its Applications in Arbitration

I. The Concept of Generative AI in the Legal Context

Artificial intelligence—defined for purposes of legal analysis—comprises adaptive computer systems capable of performing tasks associated with human cognitive capacities, including natural language comprehension, recognition of complex semantic patterns, and the generation of outputs analogous to human outputs. Generative AI in the form of Large Language Models (LLMs) such as ChatGPT-4 commands increasing attention in the international arbitration environment.

The BCLP Annual Report records that two-thirds of professionals in international arbitration now work in environments where AI tools are used in one form or another, yet the same majority expresses deep concern regarding the risks of unauthorized delegation, hallucination, and confidentiality breaches.

II. Domains of AI Deployment in Arbitration

The scope of AI deployment in arbitration extends across multiple fields: electronic discovery (e-discovery) and automated document management and classification; legal research and the

extraction of arbitral and judicial precedents from large databases such as Jus Mundi; analysis of parties' submissions and assessment of the strengths and weaknesses of each position; translation of documents in multilingual arbitrations; drafting of procedural sections of awards such as procedural history and factual background; and estimation of costs and timeframes. In the domain of predictive and forward-looking analysis, platforms such as Arbilex and Lex Machina employ statistical analysis to forecast arbitrator tendencies and map their prior decisional patterns.

Section 1.3 — Structural Tensions between the Nature of AI and the Principle of Confidentiality

I. The Data Paradox — AI's Data Hunger versus Arbitration Privacy

Generative AI tools are 'insatiably hungry for data': the wider the dataset on which a model is trained, the greater the accuracy of its outputs and the higher its predictive value. It is precisely here that the acute paradox emerges—institutional arbitration is by its nature confidential in its outcomes—awards typically remain undisclosed—making it exceedingly difficult to build an adequate database for training AI models without drawing on confidential sources. This gives rise to a dual risk: either the acquisition of sufficient data leads to a breach of confidentiality, or the model remains incapable of achieving the desired level of efficiency.

II. Risks of Data Breaches and Unauthorized Access

The risks of data breaches in AI-assisted electronic arbitration manifest in three principal forms. First, third-party breach risks: proprietary tools owned by external companies such as ChatGPT collect user input for deployment in model development, meaning that a confidential document uploaded by a lawyer to such a tool may ultimately become training material accessible to other users. Second, cybersecurity attack risks: practice has revealed the vulnerability of arbitral systems to such attacks, as evidenced by the targeting of the Permanent Court of Arbitration (PCA) website in 2015 during the maritime dispute between China and the Philippines. Third, the risk of 'hallucination' and leakage of data from prior cases: an AI model may inadvertently incorporate into its outputs elements drawn from prior legal files used in training, potentially constituting a confidentiality breach and calling into question the impartiality of the arbitral tribunal.

III. Illustrative Scenarios from Arbitral and Judicial Practice

International arbitral doctrine has posited three revealing hypothetical scenarios. In the first, counsel uses a generative AI tool to draft a memorandum summarizing evidence and arguments, whereupon the tool incorporates confidential information drawn from another client's file used in training; the opposing party discovers this and challenges the integrity of the proceedings. In the second, an arbitrator uses AI to draft the final award; the model automatically absorbs reasoning and analyses from prior awards containing sensitive commercial data of parties who were not party to the current dispute, prompting the parties to challenge the arbitrator's independence. In the third, one party uploads arbitral documents to an AI tool to prepare a chronology of events; the tool incorporates internal emails the party did not intend to disclose, leading to a dispute over admissibility of evidence and the tribunal's jurisdiction.

In actual practice, the well-known arbitration *Mikadze v. RAKIA* before the Stockholm Chamber of Commerce (SCC) generated a notable precedent when one party filed an application to set aside the award, alleging that confidential information had been breached through a third party acting on behalf of the other party.

PART TWO: THE INTERNATIONAL LEGAL AND INSTITUTIONAL FRAMEWORK — A CRITICAL ASSESSMENT

Section 2.1 — The UNCITRAL Model Law and National Legislative Frameworks

The UNCITRAL Model Law on International Commercial Arbitration was adopted as an instrument for harmonizing national legislation in this field and has been adopted or inspired by the legislation of ninety-nine states across one hundred and twenty-six jurisdictions. Yet this Law remains silent on the principle of confidentiality, containing no express provision establishing a binding obligation to that effect, as is equally the case with major national legislation. This legislative gap is reflected in the scope of arbitration proceedings governed by this Law, making the application of the law of the seat of arbitration the likely default where neither the arbitration agreement nor the rules of the arbitral institution contain a specific provision.

Article 18 of the Model Law enshrines the principle of equality between the parties and the right of each to fully present its case—a principle that itself requires that it not be undermined by confidentiality violations caused by AI tools. Article 19 grants parties' freedom to agree on the procedure, thereby providing a contractual basis for incorporating provisions governing the use of AI and the attendant confidentiality guarantees.

On a comparative level, national approaches diverge markedly: English and New Zealand courts adopt an express approach recognizing confidentiality as an implied obligation in arbitration agreements, whereas the courts of other jurisdictions deny the existence of such an obligation in the absence of an express provision or agreement. To date, no State has enacted national legislation expressly regulating the use of AI in arbitration proceedings from the perspective of confidentiality protection.

Section 2.2 — The EU AI Act and the UK AI White Paper

1. The EU AI Act 2024

The EU Artificial Intelligence Act entered into force in the summer of 2024, with full application expected by 2026. The Act adopts a risk-based approach, classifying AI systems according to their potential degree of risk and imposing stringent compliance requirements on the high-risk category.

Critically relevant in the arbitration context, Annex III, Article 8(a) of the Act classifies AI systems 'intended to be used by a judicial authority or on its behalf for researching and interpreting facts and the law and applying the law to a concrete set of facts, or used in a similar way in the context of alternative dispute resolution' within the high-risk category. This means that the deployment of AI in arbitration is likely to fall within this heightened classification.

The Act imposes on deployers—which include lawyers, arbitrators, and arbitral institutions—under Article 29, a range of obligations: establishing risk management systems, precise technical documentation of the system, adoption of appropriate human oversight measures, and compliance with robust standards of safety and accuracy. Article 78 contains an express obligation to respect the confidentiality of sensitive information and trade secrets, and to adopt effective cybersecurity measures. However, the extent to which the Act applies to third-state authorities such as the United States, the United Kingdom, and other non-EU States remains legally ambiguous and unresolved.

II. The UK AI White Paper 2023

In March 2023, the United Kingdom Government published its AI White Paper, adopting an outcomes-based approach rather than the risk-based approach of the European Regulation; meaning that the level of regulatory scrutiny is tied to the actual outcomes produced using a particular tool in a specific context. This means in practice that the use of AI in arbitration will be subject to a separate assessment depending on the nature of the task assigned to it and the degree of its potential impact. The White Paper's principles of safety, security, robustness, and interpretability are consistent with the core requirements for safeguarding confidentiality in arbitration, though they lack clearly defined binding enforcement mechanisms.

Section 2.3 — Institutional Arbitration Rules: A Comparative Study

I. ICC Arbitration Rules

The International Chamber of Commerce (ICC) Arbitration Rules take a limited and discretionary approach to confidentiality. Article 22(3) of the 2021 Arbitration Rules permits the arbitral tribunal to take measures to protect trade secrets and confidential information, but this is contingent upon a request from one of the parties and does not in itself constitute a standing obligation. Notably, the formulation of 'confidential information' in the Rules may not be sufficiently broad to encompass all documents prepared for arbitration, such as witness statements, submissions, and any materials generated through AI tools.

Given this discretionary approach, the risks arising from the use of third-party AI tools are more pronounced under the ICC framework, as the absence of clear provisions imposing confidentiality or regulating AI deployment opens the door to divergence and inconsistency in rulings.

II. LCIA Arbitration Rules

The LCIA Rules 2020 adopt a more comprehensive and stringent approach to confidentiality. Article 30 establishes a confidentiality obligation binding on the parties, the tribunal, the institution, the Registrar, and all other participants in the proceedings with respect to all documents and materials prepared for or used in the arbitration, including awards. The presumption of confidentiality operates as the default position unless the parties agree otherwise in writing. This comprehensiveness extends beyond the parties to encompass service providers, including providers of AI tools.

The LCIA Rules represent the most suitable model for addressing the challenges posed by AI compared to their counterparts; the breadth of the confidentiality obligation means that AI tool providers contracted by the parties are themselves bound by confidentiality. The Rules also permit the issuance of binding directions in the field of data protection and information security.

III. SCC Arbitration Rules

The SCC Rules 2023 take a more general approach to confidentiality. Article 3 provides that the arbitration proceedings and the award shall be kept confidential unless the parties agree otherwise; however, Swedish law—which governs many SCC proceedings—does not regard confidentiality as an implied term in arbitration agreements. This rule was expressly established in *Bulgarian Foreign Trade Bank v. AI Trade Finance* before the Swedish Supreme Court.

Although SCC issued a guidance note on the use of AI in cases administered under its rules in the final quarter of 2024, this guidance remained in a non-binding recommendation. It advises participants to be mindful of the impact of AI tools on confidentiality and to verify data processing and storage

mechanisms before use.

Section 2.4 — Specialized Guidelines: SVAMC and AAA-ICDR

I. SVAMC Guidelines on the Use of AI in Arbitration 2024

The Silicon Valley Arbitration and Mediation Center (SVAMC) issued specialized guidelines on 30 April 2024, representing the first serious and systematic attempt to close the regulatory gap in the field of AI deployment in arbitration. Principle 2 of the document expressly acknowledges the confidentiality risks associated with AI tools and obliges all participants to verify that the AI tools they use provide adequate confidentiality guarantees. It prohibits the uploading of confidential information to any tool without prior examination of its data processing and storage policies and without obtaining appropriate authorization.

However, fundamental problems call into question the effectiveness of these Principles. First, they are non-binding, carrying no legally compulsory effect; they are voluntary advisory recommendations subject to adaptation to the circumstances of each case. Second, the Principles leave participants a wide margin of discretion in dealing with confidential information after authorization has been obtained, which may open the door to third-party access to such information when AI tools are subjected to cyberattacks. Third, the Principles do not require express disclosure of AI use, though they permit the tribunal, parties, and institutions to request this in specific cases.

II. AAA-ICDR AI Principles for Alternative Dispute Resolution

The American Arbitration Association and International Centre for Dispute Resolution (AAA-ICDR) Principles adopt a more committed approach than the SVAMC Principles. Principle 2 expressly states that the use of AI in arbitration ‘should not’ result in a breach of the confidentiality obligation, and that such obligation operates independently of the will of the parties. The principles also recommend caution when dealing with large datasets and unreliable processing protocols in AI tools.

The JAMS AI Rules issued in 2024 are aligned with this orientation, providing—in Rule 16(1)—for an automatic protective order issued by the tribunal restricting access to confidential information, and requiring the presence of a neutral with technical expertise to address AI-related matters. However, these Rules are primarily directed at regulating disputes arising from the use of AI rather than the procedural framework for its deployment within arbitration proceedings.

PART THREE: TOWARDS A COMPREHENSIVE LEGAL FRAMEWORK FOR CONFIDENTIALITY PROTECTION IN THE AGE OF ARTIFICIAL INTELLIGENCE

Section 3.1 — Contractual Provisions and Procedural Confidentiality Orders

I. The Role of Party Autonomy and Contractual Provisions

Party autonomy constitutes the most original and effective legal pillar for safeguarding confidentiality against the risks of AI: the parties may contractually agree on confidentiality terms that exceed those stipulated in the institutional rules. Careful drafting requires that the arbitration agreement or the underlying contract contain provisions expressly stating that the level of confidentiality established therein extends to all information processed by or shared with AI tools; requiring prior approval from the

arbitral tribunal before any confidential document is uploaded to AI platforms; and obliging the parties to review the data processing and storage policies of the tools they intend to use. The due process requirement equally demands verification that every use of AI complies with the applicable regulations and laws at the seat of arbitration and the place of enforcement.

II. Procedural Confidentiality Orders Issued by Arbitral Tribunals

Arbitral tribunals possess, by virtue of their established procedural powers, an inherent authority to issue confidentiality orders governing the specific character of arbitration proceedings, even in the absence of express provisions in the institutional rules. The doctrinal reasoning of renowned arbitrator Gary Born confirms that the arbitral tribunal has the power to regulate procedure and to interpret the application of relevant national law to the facts of each case. In *Resolute Forest Prods. Inc. v. Canada* before the Permanent Court of Arbitration, the tribunal issued confidentiality orders protecting specific categories of evidence and materials.

The deployment of AI requires that initial procedural orders (PO1) contain provisions governing: the definition of ‘confidential information’ to encompass materials prepared for arbitration and generated by AI tools; the procedures for requesting authorization for use; data security monitoring mechanisms; and the sanctions applicable in cases of breach. The approach of the US District Court for the Eastern District of Pennsylvania—which expressly obliged parties to disclose how AI was used in the proceedings—represents a model worthy of emulation at the level of international arbitral institutions.

Section 3.2 — Proposed Model Clauses for AI-Assisted Arbitration

I. Drafting Principles and Objectives

The proposed model clause should be grounded on three core principles: obligation rather than guidance; comprehensiveness rather than selectivity; and adaptability to the rapidly evolving technological landscape. The features of this clause have been drawn from the LCIA Rules, which stand out for their superior treatment of confidentiality, while accommodating the specific considerations raised by AI tools.

II. Proposed Model Clause for AI-Assisted Arbitration

Article 10

Confidentiality and the Use of Artificial Intelligence

10.1 The parties agree that all information disclosed before and during the arbitration, including any information uploaded to or generated by artificial intelligence tools, shall be deemed confidential and subject to the applicable confidentiality obligations, save to the extent required by a legal duty, necessary to protect a right, or to seek judicial relief.

10.2 Neither party shall upload any confidential information to any artificial intelligence tool without prior approval of the arbitral tribunal. To obtain such approval, the requesting party must: (a) identify the AI tools proposed for use and furnish the tribunal with their usage policies, data processing mechanisms, and any other relevant information; (b) demonstrate that the use of such tools is a necessity demanded by and proportionate to the requirements of the arbitration; and (c) confirm that adequate measures have been taken to preserve the confidentiality of the information uploaded thereto.

10.3 The parties shall verify that any AI tools used comply with all applicable regulations and laws, including data protection and privacy legislation.

10.4 In the event of a confidentiality breach, the arbitral tribunal may impose appropriate sanctions, including the allocation of costs.

10.5 The obligations set forth in this Article shall remain in full force and effect even after the conclusion of the arbitration proceedings and the issuance of the final award.

This proposed formulation is distinguished from the SVAMC model by establishing a binding prior-approval system; requiring compliance with applicable regulations; incorporating deterrent sanctions in cases of breach; and maintaining the obligations in force after the arbitration has concluded.

Section 3.3 — ‘Confidentiality by Design’: Theoretical Basis and Practical Application

I. Theoretical Basis and Legal Reference

This research advances an original theoretical proposal grounded in the appropriation of the concept of ‘Privacy by Design’—developed by Ann Cavoukian in Canada in the early 1990s and subsequently elevated to a binding legal principle under Article 25 of the General Data Protection Regulation (GDPR)—which mandates that data protection be embedded within the design of technical systems and processes from the earliest conceptual stage, rather than appended as an administrative afterthought. By analogy with this principle, the concept of ‘Confidentiality by Design’ is advanced in the context of AI-assisted arbitration.

II. Content of the Concept and Mechanisms for Its Implementation

The concept of ‘Confidentiality by Design’ rests on the requirement that AI systems intended for deployment in arbitration be built with robust internal mechanisms protecting confidential information from unauthorized access and breaches from the moment of design rather than at a later stage. These mechanisms include advanced encryption of incoming, outgoing, and stored data; restricted access protocols grounded in the principle of genuine need-to-know; data anonymization techniques in arbitration applications; continuous audit systems to monitor and trace data flows; and time-limited retention policies preventing the indefinite retention of data.

The utility of this concept draws on an existing practical application embodied by the Jus AI platform, the ambitious AI tool of Jus Mundi, which has integrated data encryption at the core of its technical architecture and has established a partnership with Microsoft such that user queries and data are not retained by the AI provider.

III. Obstacles and Requirements for Institutionalizing the Concept

It is evident that institutionalizing ‘Confidentiality by Design’ as a settled principle encounters serious practical obstacles: major AI companies wield influence that frequently exceeds that of arbitral institutions, undermining the latter’s capacity to negotiate binding terms. Furthermore, technical standards for the design of AI systems in arbitration contexts remain nascent. The Privacy by Design principle itself required years of policy debate and complex negotiation in Europe before being codified as a binding provision in the GDPR. This research accordingly calls upon international arbitral institutions to pursue collective negotiating pathways with technology companies to elevate the requirements of confidentiality protection from the status of recommendation to the level of legal obligation.

CONCLUSION: FINDINGS AND RECOMMENDATIONS

I. Principal Findings

1. The research establishes that the use of generative AI tools owned by third-party companies in international institutional arbitration constitutes an objective threat to the principle of confidentiality, a threat that combines technical risks—such as cyberattacks and data leakage—with procedural risks, including AI hallucination and the incorporation of data from previous cases into awards.
2. The research reveals a structural deficiency in the existing international legal framework: the UNCITRAL Model Law and national legislation lack provisions addressing confidentiality in the AI context; the EU AI Act has limited application to cross-border international disputes; and institutional arbitration rules vary considerably in the comprehensiveness of their confidentiality provisions.
3. The research distinguishes three institutional patterns in addressing the confidentiality challenge: the discretionary pattern represented by the ICC; the comprehensive and express pattern represented by the LCIA; and the general and orientational pattern represented by the SCC.
4. The research concludes that specialized guidelines such as SVAMC and AAA-ICDR represent positive steps, but fall short of providing comprehensive protection by reason of their non-binding character and the absence of enforcement mechanisms.

II. Recommendations

Recommendation 1 — Strengthening Institutional Rules:

International arbitral institutions should issue updated versions of their rules containing binding and detailed provisions governing the deployment of AI in arbitration proceedings, modelled on the direction taken by the JAMS AI Rules with their automatic protective orders.

Recommendation 2 — Standardizing Initial Procedural Orders:

Arbitral tribunals should incorporate AI-specific provisions in initial procedural orders (PO1) defining the conditions and controls for authorization of AI use and the mechanisms for oversight.

Recommendation 3 — Collective Negotiation with AI Providers:

The international arbitration community—institutions, associations, and States—should negotiate collectively with major technology companies to secure binding commitments to confidentiality protection standards.

Recommendation 4 — Institutionalizing ‘Confidentiality by Design’:

This standard should be adopted as an international normative requirement for AI tools intended for deployment in arbitration, and incorporated into the practice guides and accreditation requirements of arbitral institutions.

Recommendation 5 — Revision of the UNCITRAL Model Law:

On a long-term horizon, the UNCITRAL Commission should review its Model Law to incorporate express provisions governing the deployment of AI in arbitration and establishing clear confidentiality obligations.

REFERENCES

I. Books and Academic Treatises

- [1] Born G. *International Commercial Arbitration*. Kluwer Law International. 3rd ed. 2023.
- [2] Redfern A & Hunter M. *Law and Practice of International Commercial Arbitration*. Oxford University Press. 7th ed. 2022.
- [3] Smeureanu I.M. *Confidentiality in International Commercial Arbitration*. Kluwer Law International. International Arbitration Law Library, Vol. 22. 2011.
- [4] Kurkela M & Turunen S. *Due Process in International Commercial Arbitration*. 2nd edn. 2010.
- [5] Derains Y & Schwartz E. *A Guide to the New ICC Rules of Arbitration*. The Hague. 1998.
- [6] Trakman L. Confidentiality, Privacy and Data Protection in International Commercial Arbitration. In: Ferrari F & Rosenfeld FJ (eds), *Handbook of Evidence in International Commercial Arbitration*. Kluwer Law International. 2022.

II. Journal Articles and Academic Studies

- [7] Malekela M.A. AI and Confidentiality Protection in International Commercial Arbitration: Analysis of the Existing Legal Framework. *Discover Artificial Intelligence*. Springer Nature. 2025. DOI: 10.1007/s44163-025-00316-7.
- [8] Scherer M. Artificial Intelligence in Arbitral Decision-Making: The New Enlightenment? *ICCA Congress Series* No. 21. Kluwer Law International. 2023.
- [9] Teramura N & Trakman L. Confidentiality, and Privacy of Arbitration in the Digital Era: Pies in the Sky? *Arbitration International*. 2024. DOI: 10.1093/arbint/aiae017.
- [10] Katajoki M. Arbitrator as the Deployer of an AI System. *Defensor Legis* 2/2024. 261–277.
- [11] Gore K & Karton J (eds). *Checking the Boxes: Confidentiality and Data Protection in International Arbitration*. Kluwer Arbitration. 2024.
- [12] Lagiewska M. New Technologies in International Arbitration: A Game-Changer in Dispute Resolution? *International Journal of Semiotics and Law*. 2023. DOI: 10.1007/s11196-023-10070-7.
- [13] Friedman E et al. Generative AI: Opportunities and Risks in Arbitration. *Practice Insight on International Arbitration in 2024*. Freshfields Bruckhaus Deringer. 2024.
- [14] Ajevski M et al. ChatGPT and the Future of Legal Education and Practice. *The Law Teacher*. 2023. 57(3):352–364.
- [15] Friedman D.L & Brozolo R.D. ILC International Commercial Arbitration Committee's Report and Recommendations on Confidentiality in International Commercial Arbitration. 28 *Arb. Int'l* 355. 2012.

III. Conventions, Regulations, and Guidelines

- [16] UNCITRAL Model Law on International Commercial Arbitration (as amended 2006).
- [17] Regulation (EU) 2024 on Artificial Intelligence (EU AI Act).
- [18] SVAMC Guidelines on the Use of AI in International Arbitration. 1st edn. 2024.
- [19] AAA-ICDR Principles Supporting the Use of AI in Alternative Dispute Resolution. November 2023.
- [20] JAMS AI Rules. 2024.
- [21] ICCA-NYC Bar-CPR Cybersecurity Protocol in International Arbitration. 2022.
- [22] UK Department of Science, Innovation and Technology. *A Pro-Innovation Approach to AI Regulation*. March 2023.

IV. Institutional Arbitration Rules

- [23] International Chamber of Commerce (ICC) Arbitration Rules 2021.
- [24] London Court of International Arbitration (LCIA) Rules 2020.
- [25] SCC Arbitration Institute Rules 2023.
- [26] Singapore International Arbitration Centre (SIAC) Rules 2016.
- [27] Hong Kong International Arbitration Centre (HKIAC) Rules 2018.

V. Judicial and Arbitral Decisions

- [28] *Del. Coalition for Open Gov't Inc. v. Strine*, 733 F.3d 510, 518 (3d Cir. 2013).
- [29] *Bulgarian Foreign Trade Bank Ltd v. A.I. Trade Finance Inc.*, XXVI Y.B.Com. Arb. 291 (2001) (Swedish Supreme Court).
- [30] *Mikadze and Others v. RAKIA and Others*, SCC Case No. V2018/021.
- [31] *Mata v. Avianca Airlines, Inc.*, 22-cv-1461 (PKC), US District Court, S.D.N.Y. June 22, 2023.
- [32] *Commonwealth of Australia v. Cockatoo Dockyard Pty Ltd*, [1995] 120 FLR 171, 187 (N.S.W. Ct. App.).
- [33] *Biwater Gauff (Tanzania) Ltd v. United Republic of Tanzania*, Procedural Order No. 3, ICSID Case No. Arb/05/22 (Sept 29, 2006).
- [34] *Resolute Forest Prods. Inc. v. Canada*, Confidentiality Order in PCA Case No. 2016–13 of 14 October 2016.

VI. Institutional Reports and Studies

- [35] BCLP. Two-Thirds of Legal Professionals in Favour of the Regulation of AI in International Arbitration. 13 November 2023.
- [36] Bryan Cave Leighton Paisner (BCLP). *AI in International Arbitration: The Rise of Machine Learning* (Survey Report). 2023.
- [37] Wolters Kluwer. *Future Ready Lawyer Report: Embracing Innovation, Adapting to Change*. 2023.
- [38] Mealey's International Arbitration Report. International Arbitration Experts Discuss the Impact of Artificial Intelligence on International Arbitration. 1 February 2024.

— End of Article —