Available Online: 7 April 2026 DOI: 10.54254/2753-7102/2026.32589

Legal coordination between evidence disclosure in international commercial arbitration and China's data export regulatory

Xiaoai Niu

University of Bristol, Bristol, UK

mp25150@bristol.ac.uk

Abstract. The enactment of China's Data Security Law and Personal Information Protection Law has created an issue for Chinese enterprises. It is subject to evidence production orders in overseas arbitral proceedings. The existing framework governing cross-border data transfers is procedurally ill-suited to arbitration timelines. Also, it does not address arbitration-specific scenarios. This paper employs doctrinal legal analysis to examine the interpretive scope of Article 36 of the Data Security Law. It draws on comparative references to the European Union and the United States as comparative evidence of the limits. The conflict arises because Article 36 prohibits providing data to foreign judicial or law enforcement authorities. It has not been authoritatively interpreted to exclude or include international commercial arbitral tribunals. This leaves Chinese enterprises exposed to potential administrative penalties if they produce evidence and to adverse consequences if they do not. The solution is a narrow judicial interpretation of Article 36 to exclude privately constituted commercial arbitral tribunals from its scope, accompanied by a targeted tiered classification mechanism for arbitration-specific data export applications and, as a supplementary technical measure, domestically hosted Virtual Data Rooms (VDR) for lower-sensitivity evidence production. These solutions are legally tractable and directly serve the state's interest in international commercial dispute resolution.

Keywords: international commercial arbitration, evidence disclosure, data export regulation, cross-border data flows

1. Introduction

International commercial arbitration has become the dominant mechanism for resolving cross-border commercial disputes. The electronic records generated by such transactions now constitute the primary evidentiary material in most significant proceedings [1]. Chinese enterprises participate as parties in proceedings administered by the London International Court of Arbitration, Singapore International Arbitration Centre, Hong Kong International Arbitration Centre and so forth at increasing rates [2]. They are simultaneously subject to a comprehensive domestic data protection architecture enacted through the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law [3]. The intersection of these two domains has created a compliance problem with fewer current legislative solutions.

The problem crystallises around Article 36 of the Data Security Law, which prohibits domestic organisations from providing data stored within China to foreign judicial or law enforcement authorities without prior approval from competent domestic authorities [4]. When an overseas arbitral tribunal issues a document production order, the Chinese party faces what this paper terms a double non-compliance problem. Withholding evidence risks adverse procedural consequences, including adverse inferences and sanctions [5]. Producing evidence without regulatory authorisation risks administrative penalties under Article 45 of the *Data Security Law*. Where conduct constitutes a criminal offence, a potential criminal referral [6]. The current regulatory framework for cross-border data transfers comprises the Data Exit Security Assessment Measures, the Standard Contract Measures, and the Provisions on Facilitating Cross-Border Data Flows. It addresses neither the applicable scope of Article 36 as applied to arbitral tribunals nor the timeline mismatch between its approval procedures and arbitration's disclosure deadlines [7-9].

For illustration, imagine a Chinese telecommunications company arbitrating before the London Court of International Arbitration and being compelled to produce internal network performance reports, configuration databases, and related emails. Some of these may be important data under sectoral standards promulgated by the Ministry of Industry and Information Technology [10]. Some of these may be personal information under the *Personal Information Protection Law*. If the facts of the matter meet certain thresholds, transferring these two types of information may trigger the security assessment procedure under the Data Export Security Assessment Measures. That procedure has formal timelines. In practice, it may take several weeks or more to complete [11]. This may create an awkward impasse for formal timelines, which are also measured in weeks. The company may then find itself in a conundrum. If it applies for approval, it may not meet the tribunal's deadline. If it produces the data without approval, it may risk committing a domestic crime. If it refuses to produce the data, it may invite adverse procedural consequences. This may happen in other regulated sectors. In our view, it is not a handful of exceptional cases but symptomatic of a structural gap [12].

This paper argues that the primary solution is a narrow judicial or regulatory interpretation of Article 36 which would exclude privately constituted commercial arbitral tribunals from its scope. Two supplementary mechanisms support this approach. The first is a targeted tiered classification system tuned to match typical arbitration timelines. The second is a domestically hosted VDR which doubles as a technical compliance tool for lower sensitivity evidence. This paper proceeds as follows. Section 2 analyses the conflict and its limits. The study draws on comparative references to show that existing international approaches are wanting and cannot be transplanted directly. Section 3 develops the proposed solution. Section 4 offers concluding remarks.

2. The conflict and limits

2.1. The core conflict under Chinese law

Article 36 of the *Data Security Law* prohibits the supply of data stored in the country to judicial or law enforcement authorities of foreign states without authorisation. The purpose appears deliberate. Through exercising sovereign control over the flow of data as part of the exercise of national security governance. And it also asserts sovereignty over data as a matter not subject to the extraterritorial demands of unilateral foreign public authorities [6], the interpretive question at issue is whether the international commercial arbitral tribunal constitutes a judicial authority of a foreign state under Article 36? This question has not been answered by legislative interpretation, judicial decision, or regulation by guidance. According to one stream of scholarship, invoking the contractual theory of arbitration, arbitral tribunals are private bodies granted authority to act by virtue of party agreement, and thus fall outside Article 36 [13]. A minority response recognises that arbitral awards can be enforced in 172 New York Convention Contracting States and suggests

that the interpretive question should not be closed [14, 15]. Neither conclusion has been authorised. Firms will need to thread their way past Article 36 by their own judgment, not the regulatory rod that compliance demands [16].

Article 6 of the *Personal Information Protection Law* limits personal information processing to the minimum necessary scope. It creates a tension with international arbitration's broad document production practices. Article 13 of the *Personal Information Protection Law* enumerates lawful processing bases, none of which clearly accommodates compelled production of personal data in foreign arbitration. The legal basis of Article 13(3) depends on a contested characterisation of what constitutes a legal obligation. The contract necessity basis of Article 13(2) generally covers only the data subject as the contracting party [17]. These provisions do not readily extend to embedded third-party personal data. The consequence is that even if Article 36 of the *Data Security Law* is interpreted not to apply to arbitral tribunals, production of documents containing personal information lacks a secure, lawful basis under the Personal Information Protection Law without specific regulatory amendment.

The *Data Security Law* defines important data as data whose leakage, tampering, destruction, or misuse could endanger national security, public interest and others. For enterprises in regulated sectors, the risk profile is further classified by the important data category based on Article 21 of the *Data Security Law* [4]. Sectoral instruments have been issued by the People's Bank of China and the Ministry of Industry and Information Technology. These instruments guide classifying substantial volumes of financial and industrial data as important for regulatory purposes [10, 18]. Export of important data requires prior security assessment under the Measures for the security assessment of cross-border data transfers. A procedure calibrated to neither arbitration timelines nor the specific procedural context of private commercial dispute resolution [7].

2.2. Why existing frameworks are insufficient

Neither existing Chinese regulatory mechanisms nor comparable foreign frameworks. It provides a fully workable solution for international commercial arbitration. These measures and provisions establish general approval and filing channels. However, these mechanisms do not directly address the timing and procedural requirements of arbitration. However, they do not contain any arbitration-specific points or a faster procedure to take concerning urgent disclosure requirements [7-9]. The General Data Protection Regulation of the European Union provides a legal proceedings derogation of Article 49(1)(e) of permitting transfers required to establish, exercise or defend legal claims subject to stringent necessity requirements [1]. This model however assumes the institutional framework of the European Data Protection Board and an adequacy-based transfer system. Having no Chinese equivalent makes direct transposition structurally inappropriate [19]. The United States comity-balancing practice is stated in Société Nationale Industrielle Aero Republic of the United States District Court and further evolved in the subordinate courts. This approach permits discovery notwithstanding foreign blocking statutes, subject to a case-by-case balancing of competing national interests [2]. But this framework operates as a judicial override of foreign law by the United States courts. These have no application in the context of Chinese regulatory compliance by Chinese enterprises. As the Supreme Court confirmed in Animal Science Products v. Hebei Welcome Pharmaceutical Co. in 2018, the United States court determining foreign law under Federal Rule of Civil Procedure 44.1 is not bound to defer conclusively to a foreign government's characterisation of its own law but may consider other relevant materials [3]. Accordingly, if Chinese enterprises invoking Article 36 of the *Data Security Law* in foreign proceedings should provide a detailed and particularised legal analysis. However, analysis of the current framework's interpretive ambiguity makes it difficult to formulate credibly. The comparative record thus demonstrates the limits of existing

approaches rather than models for adoption. And the solution should be developed within the Chinese regulatory framework itself.

3. A coherent response

3.1. The primary solution as interpretive narrowing of Article 36

The most legally tractable and highest-priority reform is authoritative interpretive clarification that Article 36's prohibition does not extend to international commercial arbitral tribunals constituted under recognised institutional rules to resolve private commercial disputes. The Supreme People's Court, drawing on its established practice in recognising and enforcing foreign arbitral awards under the New York Convention, occupies a certain position within China's judicial system [20]. Given its authority to issue binding judicial interpretations, it is institutionally placed to provide clarification on the scope of Article 36. Ideally developed in collaboration with the Cyberspace Administration of China. The doctrinal basis is the contractual theory of arbitration. This renders an arbitral tribunal a body with no sovereign power or power other than that which is agreed upon by the parties [21]. It is a part of another institutional alternative to the foreign courts and the state bodies [22, 23], the extraterritorial pressure of which Article 36 was meant to counter. This rationale would not suggest taking arbitral tribunals out of the scope of Article 36. It would get the prohibition in line with the real cause of regulatory fright.

The objection of the principal objection is concerned with the substantive impact. Excluding the arbitral tribunal would provide an avenue for pumping sensitive Chinese information out. As nothing can be done regarding the arbitration of commerce on internationally binding arbitral award grounds. Any elucidating tool must state that the restriction is only effective when. To begin with, the conflict is truly personal and business related. Second, the tribunal is assembled in accordance with the recognised institutional rules and has a seat. Third, document production is provably useful to the disputed issues. Fourth, there are proper confidentiality plans. These conditions make the interpretive narrowing support the compliance requirement of the enterprise as well as the data safety concern of the state. As well as coinciding with the proportionality principle that is already articulated in Article 6 of the *Personal Information Protection Law*. The issue presented by the drafting is the setting of the borders of the recognised international commercial arbitration to a enough degree. That is manageable. The practice of the New York Convention of judicial practice already deals with similar questions of definition [24].

A second objection is centred on the right avenue of clarification. The *Data Security Law* was passed by the Standing Committee of the National People's Congress [25]. In situations where judicial interpretation becomes so imperative, the legislative amendment or an interpretation by the National People's Congress of the Standing Committee is the way to go. Such an institutional objection does not have any impact on the content of the proposal but dictates how it is processed. The content of interpretation is identical according to the instrument applied. Meanwhile, regulatory guidance could be provided by the Cyberspace Administration of China in its current mandate. This advice may state that any information related to arbitration data transfer is at risk of a facilitated review route until formal clarification by law or a court.

3.2. Supporting mechanisms

Interpretive narrowing of Article 36 of the *Data Security Law* resolves the threshold question of regulatory authorisation. But does not address the *Personal Information Protection Law*'s lawful basis problem for personal data. And the classification problem for important data, or the timeline mismatch for regulated-sector enterprises. Two supplementary mechanisms address these residual issues.

First, a targeted tiered classification mechanism. Building on the Data Security Law's existing data classification architecture and the "Data security technology—Rules for data classification and grading" (GB/T 43697-2024 standard) [26], such as ordinary commercial data, contractual documents, correspondence, and financial records do not involve important data or national security concerns. They could be presumptively producible in international arbitration, subject to post-production notification. Parties should be encouraged to address evidence production protocols in pre-arbitration contractual data security clauses. For data containing personal information, arbitral production orders may be interpreted as creating a legal obligation under Article 13(3) of the *Personal Information Protection Law*. Alternatively, as a medium-term objective, a formal legislative amendment could introduce a legal proceedings exception analogous to Article 49(1)(e) of the *General Data Protection Regulation*, thereby providing the secure lawful basis that currently does not exist. For important data, the existing prior approval requirement should be maintained. However, an expedited review procedure could be envisaged for arbitration applications, with arbitration bodies empowered to provide supporting documentation to accompany applications and assist the competent authority in conducting timely assessments. The mechanism's biggest shortcoming is sequencing. The personal information exception cannot be enacted by legislation, which is likely to be glacial. An important data expedited review procedure requires persistent inter-agency coordination that has proven challenging in the past. We therefore recommend proceeding with the mechanism in parallel with, not as a substitute for interpretive clarification.

Second, domestically hosted VDRs are a technical complement. A VDR hosted on servers located in Chinese territory, which arbitrators and opposing counsel can use to remotely review documents that are not downloaded or retained locally. It provides a basis to argue that there is no cross-border data transfer. This argument has legal force under the contractual theory of arbitration. It is aided by the trend of reviewing evidence remotely in international arbitration following the COVID-19 pandemic. The risk is that the Cyberspace Administration of China is developing a response to the definition of data export. Whether foreign persons' remote access to data stored in China constitutes a potential data export on some, though not all, occasions is unsettled. The VDR model should accordingly be deployed as a supplementary risk-reduction tool for lower-sensitivity commercial data, not as a standalone compliance pathway. It becomes a primary compliance mechanism. Only if the Cyberspace Administration of China explicitly endorses VDR-based remote access as consistent with localisation requirements. This endorsement is an outcome that the paper's proposal could facilitate.

4. Conclusion

The conflict between arbitral evidence disclosure obligations and China's data export regulatory framework is structural. It cannot be fully resolved through interpretive clarification alone. Chinese enterprises may face a double non-compliance dilemma. When arbitral production orders intersect with Article 36 of the *Data Security Law*. The current regulatory architecture provides no structured solution. Existing cross-border data transfer mechanisms are procedurally misaligned with typical arbitration timelines. The *Personal Information Protection Law* provides no clear lawful basis for arbitration-driven personal data production. The important data regime imposes approval obligations. That may not be met within an arbitration's procedural calendar.

This paper argues that the primary solution is a narrow interpretive clarification of Article 36. This way excludes privately constituted commercial arbitral tribunals from its scope. Minimum safeguards, such as relevance, confidentiality, and institutional recognition, should accompany this approach. This reform is legally tractable. It requires no legislative amendment. It also draws on doctrinal foundations in the contractual theory of arbitration and existing Supreme People's Court practice under the New York Convention.

Furthermore, it is consistent with Chinese policy interests in participating in international commercial dispute resolution. A regulatory posture that enforces broad data export restrictions may hinder legitimate arbitral evidence production. Where relevant evidence cannot be transferred, Chinese parties could face disadvantages in foreign proceedings. It may also signal to foreign counterparties that data-intensive disputes involving Chinese enterprises carry procedural risks. These perceptions could, in turn, affect the attractiveness of Chinese arbitral institutions. However, these consequences are not necessarily required by the data sovereignty rationale.

The supporting mechanisms could be envisaged. A tiered classification approach could provide a more secure regulatory pathway for different data categories. In parallel, domestically hosted VDR may serve as a technical complement for lower-sensitivity evidence. These mechanisms aim to address residual issues that interpretive clarification alone is unlikely to resolve. Both mechanisms, however, face practical implementation constraints. The tiered approach may require further legislative or regulatory clarification for the personal information component, as well as inter-agency coordination for the important data component. The legal position of VDR models also remains unsettled in the absence of clear regulatory guidance. Particularly as regards whether remote access constitutes a restricted form of data export. These constraints support pursuing the reforms in parallel, and with a degree of urgency, rather than abandoning them. Of the two, the tiered classification approach is arguably more structurally significant, as it engages the full range of data categories implicated in arbitration. By contrast, Future research could examine VDR models that might be more readily deployable as an interim technical measure while legislative and regulatory processes continue to develop.

Notes

1. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1.

2. Société Nationale Industrielle Aérospatiale v United States District Court 482 US 522 (1987)

3. Animal Science Products, Inc. v. Hebei Welcome Pharmaceutical Co. Ltd., 585 U.S. _ (2018).

References

[1] Ferreira, D.B., & Gromova, E.A. (2023). Electronic evidence in arbitration proceedings: Empirical analysis and recommendations. *Deakin Law School Research Journal, 20*, 30-39. https: //doi.org/10.14296/deeslr.v20i.5608

[2] Chu, B., & Wang, W. (2022). Building an international arbitration hub: China's competitiveness and direction. *Frontiers in Marine Science, 9*, 1-15. https: //doi.org/10.3389/fmars.2022.986617

[3] Creemers, R. (2021). China's emerging data protection framework. *SSRN Electronic Journal*, 1–25. https: //doi.org/10.2139/ssrn.3964684

[4] National People's Congress. (2021). *Data Security Law of the People's Republic of China*. http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html

[5] Grant, A., Kleist, P., Molfa, M., & Wen Wei, A. (2019). Challenges in the taking of evidence in arbitrations seated in mainland China. *Journal of International Arbitration, 36*(3), 315-336. https: //kluwerlawonline.com/journalarticle/Journal+of+International+Arbitration/36.3/JOIA2019015

[6] Wang, J. (2025). *Transferring data to foreign authorities under Chinese data protection law.* International Data Privacy Law, ipaf026. https: //doi.org/10.1093/idpl/ipaf026

[7] Cyberspace Administration of China. (2022). *Measures for security assessment of cross-border data transfers*. https://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm

[8] Cyberspace Administration of China. (2023). *Measures on standard contracts for the cross-border transfer of personal information*. https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzbmgz/202306/t20230620_481044.html

[9] Cyberspace Administration of China. (2024). *Provisions on promoting and regulating cross-border data flows.* https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzbmgz/202410/t20241030_508738.html

[10] Ministry of Industry and Information Technology. (2022). *Industrial data classification and grading guidelines (trial)*. https://www.gov.cn/zhengce/zhengceku/2020-03/07/content_5488251.htm

[11] Liu, J. (2023). China's security assessment measures for outbound data transfers. *Journal of East Asia and International Law, 16*(2), 267–282. https: //doi.org/10.14330/jeail.2023.16.2.04

[12] Tianchan, R. (2025). Navigating the complexities of extraterritorial application of jurisdiction in data protection laws. *Peking University Law Journal, 13*(1), 123–144. https: //doi.org/10.1080/20517483.2025.2561309

[13] Tehrani, M., & Bagelan, L. (2025). Examination of legal theories on the nature of international commercial arbitration with an approach to the source of the arbitrator's authority. *The Encyclopedia of Comparative Jurisprudence and Law,* 1–17. https: //doi.org/10.61838/jecjl.275

[14] Fu, T. K. M., Yang, R. C. L., & Zhou, E. J. S. (2024). *Cross-border transfer of evidence from mainland China under international commercial dispute resolution scenarios*. Mayer Brown LLP. https://www.lexology.com/library/detail.aspx?g=3eb3f703-44b0-422f-a532-b121e11bd8c4

[15] Crowell & Moring LLP. (2025). *Cross-border data, rising risks: How international arbitration can help.* https: //www.crowell.com/en/insights/client-alerts/cross-border-data-rising-risks-how-international-arbitration-can-help

[16] Chen, J., & Sun, J. (2021). Understanding the Chinese data security law. *International Cybersecurity Law Review, 2*, 209–221. https: //doi.org/10.1365/s43439-021-00038-3

[17] National People's Congress. (2021). *Personal Information Protection Law of the People's Republic of China*. http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html

[18] People's Bank of China. (2020). *Financial data security: Data classification and grading guidelines.* https://std.samr.gov.cn/hb/search/stdHBDetailed?id=B081D125A6762DB8E05397BE0A0A5EA7

[19] Panek, W. (2024). People's Republic of China and the adequacy: Why Chinese data protection law is not adequate within the meaning of the GDPR. *Masaryk University Journal of Law and Technology, 18*(2), 143–167. https: //doi.org/10.5817/MUJLT2024-2-1

[20] Liu, S. (2025). Research on the current situation and countermeasures of international commercial arbitration in China. *Economics, Law and Policy, 8*(2), 162. http: //dx.doi.org/10.22158/elp.v8n2p162

[21] Godhe, A. (2025). Characterisation of rules in international commercial arbitration: Between procedure, substance and party autonomy. *International Journal for the Semiotics of Law*. https: //doi.org/10.1007/s11196-025-10369-7

[22] Blackaby, N., Partasides, C., Redfern, A., & Hunter, M. (2015). *Redfern and Hunter on international arbitration* (6th ed.). Oxford University Press. https://doi.org/10.1093/law/9780198714248.001.0001

[23] Teramura, N., & Trakman, L. (2024). Confidentiality and privacy of arbitration in the digital era: pies in the sky? *Arbitration International, 40*(3), 277–306. https: //doi.org/10.1093/arbint/aiae017

[24] Kronke, H., Nacimiento, P., Otto, D., & Port, N. C. (Eds.). (2024). *Recognition and enforcement of foreign arbitral awards: A global commentary on the New York Convention.* Kluwer Law International.

[25] Standing Committee of the National People's Congress. (2023). *Legislation Law of the People's Republic of China (2023 Amendment).* https://dzb.mju.edu.cn/2023/0320/c3927a146042/page.htm

[26] State Administration for Market Regulation, & Standardisation Administration of the People's Republic of China. (2024). *Data security technology — Rules for data classification and grading (GB/T 43697-2024)*. National Public Service Platform for Standards Information.