Vol. 3 No.3 2025

RECOGNIZED IN "Y" CATEGORY BY

Research Consortium Archive
P(ISSN) : 3007-0031
E(ISSN) : 3007-004X
https://rc-archive.com/index.php/Journal/about

Cross-Border Data Transfers and Trade Secrecy in International Commercial Arbitration

Dr. Khurram Baig
University Gillani Law College, BZU Multan
Email: mkb5729@gmail.com

Jawad khalil Pitafi
Operational Officer
Companies House, United Kingdom
(Uk Civil Services)
Email:Jawadkhalilpitafi@gmail.com

Muhammad Ahsan Iqbal Hashmi*
Assistant Professor of Law
Bahauddin Zakariya University, Mulan (Vehari Campus)
Email: ahsanhashmi@bzu.edu.pk

Publisher : EDUCATION GENIUS SOLUTIONS
Review Type: Double Blind Peer Review

ABSTRACT

The rapid digitization of global commerce has introduced complex legal challenges into the domain of international commercial arbitration, particularly in relation to cross-border data transfers and the protection of trade secrets. Arbitration, traditionally valued for its confidentiality, now confronts a rapidly evolving regulatory landscape shaped by competing national laws on data protection, digital sovereignty, and cybersecurity. This paper critically examines how international arbitral proceedings are impacted by legal regimes such as the European Union's General Data Protection Regulation (GDPR), the U.S. CLOUD Act, and emerging data localization mandates across Asia and Africa. These frameworks not only complicate the lawful transfer and storage of sensitive information across jurisdictions but also risk undermining core procedural safeguards in arbitration.

The research investigates how trade secrets—such as proprietary algorithms, source code, customer databases, and financial models—can be effectively protected within arbitral processes that involve parties, institutions, or data located in multiple legal regimes. It evaluates the existing safeguards under leading institutional rules, including those of the ICC, LCIA, SIAC, and HKIAC, and assesses the adequacy of confidentiality protocols, protective orders, and data security measures.

Drawing on doctrinal analysis and comparative legal methodology, this study identifies several areas of vulnerability: inconsistent enforcement of confidentiality obligations across borders, lack of standard technical protocols for secure data transmission, and ambiguities in arbitrator duties related to data handling. The paper further explores how arbitral tribunals and institutions can integrate cybersecurity frameworks, use secure digital platforms, and adopt harmonized guidelines to navigate these cross-jurisdictional risks. Recommendations are made for reforming institutional rules, adopting model clauses on data protection, and enhancing arbitrator training in digital evidence and cybersecurity.

Ultimately, this research contends that the legitimacy and functionality of international arbitration in the digital era depend on a careful balance between confidentiality, data protection, and procedural transparency. By addressing the dual imperatives of protecting trade secrets and respecting divergent data governance regimes, this paper proposes a forward-looking legal framework capable of sustaining arbitration's role in resolving high-value, cross-border commercial disputes in the information age.

Keyword: Cross-border data transfers, Trade Secrets, International Arbitration, Confidentiality, Data Protection, Cybersecurity, Institutional Rules, Digital Sovereignty.

Introduction

In an era dominated by digitization and globalization, data has become a pivotal asset in cross-border commercial transactions. International commercial arbitration, the preferred dispute resolution mechanism for multinational corporations, is increasingly required to address disputes involving sensitive business information, proprietary technologies, and trade secrets. This evolution has prompted concerns over how arbitral proceedings, often seated in diverse jurisdictions and involving electronically stored information (ESI), manage data that may be subject to conflicting legal regimes governing cross-border transfers and confidentiality.[1]

[1] Christopher Millard and Christopher Millard, eds., *Cloud Computing Law*, Second Edition, Second Edition (Oxford University Press, 2021).

Trade secrets—defined broadly as any information that derives economic value from not being generally known and that is subject to reasonable steps to keep it secret—are often at the heart of commercial disputes. Yet their protection in arbitration faces complex legal and procedural challenges. These challenges become more pronounced when data must cross borders, triggering privacy laws such as the EU's General Data Protection Regulation (GDPR), the U.S. CLOUD Act, or data localization laws in jurisdictions like China, India, or Russia.[2] These legal frameworks create a fragmented landscape that may limit or complicate the transfer of trade-secret-laden data across borders for arbitration purposes.[3]

Moreover, the private nature of arbitration is both an opportunity and a liability in this context. While confidentiality is a hallmark of arbitration, it is not synonymous with secrecy, and the procedural mechanisms for protecting trade secrets vary considerably among arbitral institutions. With tribunals lacking coercive powers and operating under different institutional rules, the risk of inadvertent disclosure or jurisdictional non-compliance is significant.[4]

This paper examines the legal complexities surrounding cross-border data transfers and trade secrecy within international arbitration. It assesses how current arbitral rules, institutional guidelines, and international legal instruments respond to these challenges. The paper also explores the emerging role of cybersecurity protocols, protective orders, and data localization trends in shaping arbitral practice. By identifying both gaps and best practices, this study aims to contribute to the development of harmonized approaches to safeguard confidential commercial information in transnational arbitration contexts.[5]

Legal Framework Governing Cross-Border Data Transfers

Cross-border data transfers form the backbone of global commerce and international arbitration. However, they are tightly regulated by national and supranational laws aimed at safeguarding personal data and national interests. These regulations pose significant legal challenges for arbitration proceedings, especially when sensitive or confidential data must be shared across jurisdictions. The variance among national laws has led to a patchwork of legal standards that often conflict or overlap, thereby complicating the arbitral process.

The European Union's General Data Protection Regulation (GDPR) remains the most comprehensive and influential data protection regime in the world. It prohibits data transfers outside the EU unless the destination country ensures an adequate level of protection or other specific safeguards are in place.[6] This directly impacts arbitral tribunals and parties operating from or engaging with EU-based entities. Compliance with GDPR may require mechanisms such as Standard Contractual Clauses (SCCs) or

[2] W. Gregory Voss, "Cross-Border Data Flows, the GDPR, and Data Governance," *Washington International Law Journal* 29 (2020 2019): 485.

[3] Gabrielle Kaufmann-Kohler and Michele Potestà, *Investor-State Dispute Settlement and National Courts: Current Framework and Reform Options*, European Yearbook of International Economic Law (Springer International Publishing, 2020), https://doi.org/10.1007/978-3-030-44164-7.

[4] "A Research on Confidentiality in Arbitration 4 Issue 5 Indian Journal of Law and Legal Research 2022," accessed July 29, 2025, https://heinonline.org/HOL/LandingPage?handle=hein.journals/injlolw8&div=23&id=&page=.

[5] "A Research on Confidentiality in Arbitration 4 Issue 5 Indian Journal of Law and Legal Research 2022."

[6] "A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergences 13 Hastings Science and Technology Law Journal 2022," accessed July 29, 2025, https://heinonline.org/HOL/LandingPage?handle=hein.journals/hascietlj13&div=12&id=&page=.

Binding Corporate Rules (BCRs), both of which were affirmed by the European Court of Justice in the *Schrems II* decision, which invalidated the Privacy Shield agreement with the U.S.[7]

In contrast, the U.S. approach to data governance, particularly under the Clarifying Lawful Overseas Use of Data (CLOUD) Act, adopts a more security-centric approach, allowing law enforcement access to data stored abroad by American service providers. This extraterritorial reach may raise alarms in arbitration involving U.S. entities, as the data under arbitration may be susceptible to government seizure despite confidentiality obligations.[8]

Meanwhile, China's Data Security Law (DSL) and Personal Information Protection Law (PIPL), both enacted in 2021, impose strict restrictions on data exports, particularly where the data concerns "critical information infrastructure" or may affect "national security." These laws impose heavy compliance burdens on foreign arbitral institutions operating in or dealing with China.[9] Similarly, countries like India and Russia have introduced data localization laws that mandate the storage and processing of data within their national territories, severely restricting international data flow.

The lack of harmonization among these regimes creates not only legal uncertainty but also significant compliance costs for arbitration users. Arbitral institutions and tribunals must now grapple with an added layer of data governance obligations, often without a coherent global legal framework to guide them.[10] The challenges become especially acute when trade secrets or confidential commercial data are involved, as parties must ensure both legal compliance and protection from competitive harm.

Trade Secrecy in Arbitration Proceedings

Trade secrecy forms a critical element in many commercial disputes, especially in sectors involving technology, pharmaceuticals, and intellectual property. In international commercial arbitration, parties often rely on arbitration's promise of confidentiality to protect such secrets from public disclosure. However, the treatment of trade secrets in arbitral proceedings varies widely and remains a subject of evolving concern, particularly in the digital age.

Trade secrets are generally defined as information that derives independent economic value from not being generally known and is subject to reasonable efforts to maintain its secrecy. This concept is now formally recognized in several international instruments, such as the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, which obligates World Trade Organization (WTO) members to provide legal protection for undisclosed information.[11] Furthermore, the 2016 EU Trade Secrets Directive harmonizes protection across EU Member States, influencing

---

[7] Nandini Singh, "Schrems II: Impact on International Exchange of Personal Data," *Indian Journal of Law and Legal Research* 5 Issue 1 (2023): 1.

[8] "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (Second Edition) by Ian Walden :: SSRN," accessed July 29, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4227129.

[9] "China's Personal Information Protection Law and Its Global Impact – The Diplomat," accessed July 29, 2025, https://thediplomat.com/2021/08/chinas-personal-information-protection-law-and-its-global-impact/.

[10] "Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance | Interdisciplinary Studies in Society, Law, and Politics," accessed July 29, 2025, http://193.36.85.187:8089/index.php/isslp/article/view/309.

[11] David Ike, "PRESERVATION OF TRADE SECRETS PURSUANT TO TRIPS AGREEMENT AND EMERGING NATIONS," *Nnamdi Azikiwe University, Awka Journal of Public and Private Law* 11, no. 0 (2021): 0, https://ezenwaohaetorc.org/journals/index.php/UNIZIKJPPL/article/view/1670.

arbitration involving European parties.[12]

Confidentiality is often cited as a key feature of arbitration. However, it is not uniformly guaranteed under all arbitral regimes. Some institutional rules (such as those of the International Chamber of Commerce (ICC) and the London Court of International Arbitration (LCIA)) contain express provisions on confidentiality, while others leave it to the discretion of the tribunal or the parties' agreement. This discrepancy raises risks for parties seeking to preserve the integrity of trade secrets during proceedings.[13]

A major concern is the handling of evidentiary disclosure in arbitration. Unlike litigation, arbitration may permit broader evidentiary production, and in some cases, tribunals may order the disclosure of documents containing sensitive trade information. Balancing the parties' right to a fair hearing with the need to protect proprietary information remains a challenging endeavor. Arbitral tribunals may resort to procedural tools such as confidentiality orders, in camera hearings, or the use of confidentiality rings to manage this tension.[14]

The International Bar Association (IBA) Rules on the Taking of Evidence in International Arbitration (2020) provide useful, though non-binding, guidance in this regard. Article 9.3 allows tribunals to exclude evidence on grounds of commercial or technical confidentiality, reinforcing protection mechanisms for trade secrets. However, these protections are not absolute and vary depending on the tribunal's interpretation, making enforcement inconsistent across cases.[15]

As arbitration increasingly involves cloud-based communication and electronic submission of documents, the risk of data leaks and unauthorized access further complicates the protection of trade secrets. This raises the importance of cyber-protocols and robust digital safeguards during proceedings, especially where sensitive technical information is concerned.

Challenges in Protecting Trade Secrets Across Jurisdictions

Trade secrets, while crucial for preserving competitive advantage in global commerce, face significant vulnerability when subjected to cross-border arbitration. Unlike patents or trademarks, trade secrets lack registration, making their legal protection highly dependent on national laws. This leads to serious inconsistencies in enforcement, especially in arbitration involving multiple legal systems with divergent approaches to confidentiality, evidence, and digital security.

One key challenge lies in the fragmented nature of trade secret protection globally. While some jurisdictions like the United States have codified trade secret law through instruments like the Defend Trade Secrets Act (DTSA) of 2016, others rely heavily on general principles of tort or contract law. This divergence becomes problematic when an arbitral tribunal must weigh conflicting laws concerning disclosure or protective

[12] "Evolving Paradigms of Trade Secret Protection: A Comparative Study of the US, EU, and India | Trends in Intellectual Property Research," accessed July 29, 2025, https://iprtrends.com/TIPR/article/view/32.

[13] Fabian Junge, "The Necessity of European Harmonization in the Area of Trade Secrets," SSRN Scholarly Paper no. 2839693 (Social Science Research Network, September 16, 2016), https://doi.org/10.2139/ssrn.2839693.

[14] "Chapter 6: Arbitration - the Chamber of Secrets? An Analysis of Procedural Rules and Technical Tools for the Protection of Trade Secrets in Arbitration in: Research Handbook on Intellectual Property Rights and Arbitration," accessed July 29, 2025, https://www.elgaronline.com/edcollchap/book/9781800378360/book-part-9781800378360-15.xml.

[15] "MediaHandler (1)," n.d.

measures.[16]

Complicating matters further, arbitral tribunals do not possess sovereign enforcement powers. Enforcement of confidentiality orders—particularly in cases involving parties from different jurisdictions—can be severely hampered by domestic court reluctance or procedural incompatibilities. The New York Convention (1958) governs the recognition of arbitral awards, but it offers limited guidance on enforcing interim confidentiality or protective orders related to trade secrets.[17]

Cybersecurity risks represent another layer of vulnerability. Given the digital nature of many trade secrets—ranging from source codes to business processes—the transmission, storage, and sharing of sensitive data during arbitration proceedings expose parties to hacking, unauthorized leaks, or cross-border data seizure. This is particularly concerning in arbitrations involving jurisdictions with extraterritorial data access laws, such as the U.S. CLOUD Act or Chinese Data Security Law, both of which permit government access to foreign-stored data under certain conditions.[18]

Moreover, data localization laws and regulations on cross-border data transfer, such as the General Data Protection Regulation (GDPR) in the EU, add further complexity. These laws may prohibit the unrestricted transfer of sensitive data—including trade secrets—outside their jurisdiction without adequate safeguards. Arbitrators, especially those unfamiliar with data protection regulations, may inadvertently order measures that contravene these local data laws.[19]

Arbitral institutions and parties are now increasingly resorting to data protection protocols and specific procedural rules to address these gaps. However, the lack of standardization across arbitral regimes means that such protocols vary widely in effectiveness. There remains a pressing need for convergence in how trade secrets are protected across borders to avoid undermining the legitimacy of arbitration as a safe venue for resolving sensitive disputes.[20]

Arbitral Tribunal Powers and Institutional Rules

The ability of arbitral tribunals to effectively manage and safeguard trade secrets hinges on both their discretionary authority and the procedural frameworks established by arbitral institutions. As cross-border disputes increasingly involve proprietary information and sensitive digital data, the institutional rules and the tribunal's proactive role have become essential in balancing fairness with confidentiality.

Most leading arbitral institutions—such as the International Chamber of Commerce (ICC), the London Court of International Arbitration (LCIA), and the Singapore International Arbitration Centre (SIAC)—have incorporated confidentiality provisions into their rules. For example, Article 22 of the LCIA Arbitration Rules (2020)

[16] "Cases and Materials on Trade Secret Law | Elizabeth A. Rowe | 1656726 | University of Virginia School of Law," accessed July 29, 2025, https://www.law.virginia.edu/scholarship/publication/elizabeth-rowe/1656726.

[17] "A Critical Analysis: Nuances of Interim Relief in International Commercial Arbitration 5 Jus Corpus Law Journal 2024-2025," accessed July 29, 2025, https://heinonline.org/HOL/LandingPage?handle=hein.journals/juscrp5&div=22&id=&page=.

[18] "Arbitration in Cross-Border Data Protection Disputes | Journal of International Dispute Settlement | Oxford Academic," accessed July 29, 2025, https://academic.oup.com/jids/article/15/4/534/7758207.

[19] Nicoleta Stelea and Gavrila Calefariu, "International Arbitration and GDPR Application," *Romanian Arbitration Journal / Revista Romana de Arbitraj* 18 (2024): 75.

[20] "Arbitration in the Age of Blockchain," accessed July 29, 2025, https://umontreal.scholaris.ca/items/c1356514-72cb-439a-975e-9b064a9974ac.

empowers tribunals to take measures to protect confidential information, including issuing directions on document access, storage, and non-disclosure obligations.[21] The SIAC Technology Disputes Protocol (2021) also provides optional protocols for information security, which may be adopted to address trade secrecy risks, particularly in tech-heavy disputes.[22]

However, these institutional rules vary widely in their strength and enforceability. While the International Centre for Settlement of Investment Disputes (ICSID) and UNCITRAL rules provide mechanisms for confidentiality, they often leave much discretion to the parties or tribunals, resulting in inconsistent protective standards. In practice, the lack of harmonized criteria for when and how to apply confidentiality measures leads to fragmented outcomes, especially in multiparty or investor-state disputes where trade secrets may be tangentially implicated.[23]

Tribunals may also issue procedural orders establishing confidentiality protocols tailored to the dispute at hand. These orders may define who may access sensitive documents, establish secure data rooms, restrict the use of information in subsequent litigation, or even designate neutral experts to review documents without full disclosure to opposing parties. While effective in theory, such orders are dependent on voluntary compliance, as tribunals lack coercive enforcement powers absent judicial support.[24]

Some arbitration practitioners advocate for the broader use of model protective orders and cybersecurity protocols, such as those developed by the International Council for Commercial Arbitration (ICCA), the New York City Bar Association, and CPR Institute. These tools provide templates for arbitrators and counsel to protect data integrity and confidentiality proactively. Nonetheless, their adoption remains voluntary and not all institutions mandate their use, which limits their systematic impact.[25]

Given the increasing complexity of cross-border data and the prevalence of trade secrets in disputes, future reforms may benefit from embedding standardized confidentiality frameworks into institutional rules. Empowering tribunals with clearer procedural mechanisms and ensuring cross-jurisdictional enforceability would go a long way in making arbitration a truly secure venue for sensitive commercial matters.

Proposals for Reform and Best Practices

Given the globalized nature of arbitration and the increasing prevalence of data-driven disputes, the current fragmented approach to trade secret protection and cross-border data transfers in arbitration is no longer sufficient. Legal scholars and institutions have proposed multiple reforms to enhance the integrity, consistency, and enforceability of data protection and trade secrecy safeguards in arbitral proceedings.

One major reform proposal is the development of harmonized guidelines or a soft law

[21] "LCIA Arbitration Rules 2020," accessed July 29, 2025, https://www.lcia.org/Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx.

[22] "SIAC Rules 2025 - Singapore International Arbitration Centre," accessed July 29, 2025, https://siac.org.sg/siac-rules-2025.

[23] Esmé Shirlow, "Transparency in Investment Treaty Arbitration: Past, Present, and Future," *Journal of International Dispute Settlement* 16, no. 3 (2025): idaf019, https://doi.org/10.1093/jnlids/idaf019.

[24] Nobumichi Teramura and Leon Trakman, "Confidentiality and Privacy of Arbitration in the Digital Era: Pies in the Sky?," *Arbitration International* 40, no. 3 (2024): 277–306, https://doi.org/10.1093/arbint/aiae017.

[25] "The ICCA Reports No. 6: ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration | ICCA," accessed July 29, 2025, https://www.arbitration-icca.org/icca-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration.

instrument that can be adopted across arbitral institutions. Such guidelines would standardize minimum safeguards for handling trade secrets and personal or sensitive data. Drawing inspiration from the IBA Rules on the Taking of Evidence in International Arbitration, a unified protocol on trade secrecy and data handling could include default clauses on redaction, in-camera review, and cybersecurity obligations.[26]

A second proposal involves embedding default data protection standards into arbitration rules themselves. For example, arbitral institutions could impose mandatory encryption, digital access control systems, and anonymization for sensitive filings. These standards would draw on best practices from data privacy regimes such as the EU's General Data Protection Regulation (GDPR) and the OECD Privacy Guidelines, without making tribunals responsible for enforcement of national laws.[27]

Another reform concerns the designation of data confidentiality officers or expert neutrals. Much like technical experts in patent or construction disputes, these professionals would oversee data handling and advise tribunals on appropriate protective measures. Their involvement would ensure that arbitrators without technical backgrounds do not overlook critical risks to trade secrecy or data integrity.[28]

The use of blockchain technology for secure document exchange and time-stamping has also been suggested, particularly for high-stakes commercial disputes involving parties from jurisdictions with divergent cybersecurity standards. Blockchain-based solutions can create tamper-proof logs, provide controlled access, and ensure data integrity without reliance on a central authority—aligning well with the decentralized nature of arbitration.[29] However, these technologies must be integrated with caution, ensuring they do not inadvertently undermine party autonomy or procedural flexibility.

Finally, capacity-building for arbitrators, counsel, and institutions is essential. Regular training in data governance, emerging technologies, and information security can raise the baseline competence of all arbitration participants. Institutions like the Chartered Institute of Arbitrators (CIArb) and ICC's Institute of World Business Law are already offering such programs, but their uptake should be broadened and incentivized globally.[30]

Incorporating these reforms would allow international arbitration to remain a preferred dispute resolution mechanism for complex commercial disputes in the digital age—ensuring that trade secrets and cross-border data flows are respected, protected, and efficiently managed within the arbitral process.

Conclusion

The evolving dynamics of global commerce and the digitization of business processes have redefined the contours of international commercial arbitration. In particular, the

[26] "The 2020 Revisions to the IBA Rules of Evidence | International Bar Association," accessed July 29, 2025, https://www.ibanet.org/2020-revisions-to-IBA-rules-of-evidence-neuhaus-voser.

[27] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, February 11, 2002, https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.

[28] Fabricio Fortese and Sophie Nappert, "Assessing Expert Evidence," SSRN Scholarly Paper no. 4976523 (Social Science Research Network, April 1, 2025), https://papers.ssrn.com/abstract=4976523.

[29] Yigit Efe Dincer, *Arbitration in the Age of Blockchain*, April 2024, http://hdl.handle.net/1866/33059.

[30] "Ciarb | Courses," accessed July 29, 2025, https://www.ciarb.org/courses/.

legal management of cross-border data transfers and the protection of trade secrets have emerged as complex yet essential issues requiring urgent doctrinal and procedural clarity. While confidentiality has long been a defining feature of arbitration, the intrusion of new legal regimes—such as data localization laws, privacy regulations, and cybersecurity standards—demands a recalibration of how arbitral tribunals treat sensitive information.

This research has demonstrated that international arbitration operates within a fragmented regulatory environment where overlapping jurisdictions and inconsistent institutional rules create challenges for effective protection of trade secrets and data. Existing frameworks like the GDPR and institutional rules such as those of the ICC and LCIA provide some procedural safeguards, but lack a uniform and enforceable approach. The divergence in national laws and the extraterritorial reach of legislation such as the U.S. CLOUD Act exacerbate uncertainty for parties engaging in arbitration across borders.

Addressing these gaps requires a multi-pronged strategy. Harmonization efforts through model rules or soft law instruments, coupled with technological interventions like secure digital platforms and blockchain integration, offer pragmatic solutions. Moreover, embedding data security protocols into institutional rules and increasing arbitrator competence through specialized training can reinforce the procedural integrity of arbitral proceedings.

Ultimately, the legitimacy and effectiveness of international commercial arbitration in the data-driven economy will depend on its ability to adapt to the dual imperatives of protecting trade secrecy and respecting data sovereignty. As cross-border commercial disputes become more frequent and complex, the arbitration community must proactively develop legal, procedural, and technological tools to preserve confidentiality without compromising transparency, fairness, or enforceability. The future of international arbitration lies in this balance—where legal innovation meets technological resilience.

References

"A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergences 13 Hastings Science and Technology Law Journal 2022." Accessed July 29, 2025. https://heinonline.org/HOL/LandingPage?handle=hein.journals/hascietlj13&div=12&id=&page=.

"A Critical Analysis: Nuances of Interim Relief in International Commercial Arbitration 5 Jus Corpus Law Journal 2024-2025." Accessed July 29, 2025. https://heinonline.org/HOL/LandingPage?handle=hein.journals/juscrp5&div=22&id=&page=.

"A Research on Confidentiality in Arbitration 4 Issue 5 Indian Journal of Law and Legal Research 2022." Accessed July 29, 2025. https://heinonline.org/HOL/LandingPage?handle=hein.journals/injlolw8&div=23&id=&page=.

"Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (Second Edition) by Ian Walden :: SSRN." Accessed July 29, 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4227129.

"Arbitration in Cross-Border Data Protection Disputes | Journal of International Dispute Settlement | Oxford Academic." Accessed July 29, 2025. https://academic.oup.com/jids/article/15/4/534/7758207.

"Arbitration in the Age of Blockchain." Accessed July 29, 2025. https://umontreal.scholaris.ca/items/c1356514-72cb-439a-975e-9b064a9974ac.

"Cases and Materials on Trade Secret Law | Elizabeth A. Rowe | 1656726 | University of Virginia School of Law." Accessed July 29, 2025. https://www.law.virginia.edu/scholarship/publication/elizabeth-rowe/1656726.

"Chapter 6: Arbitration - the Chamber of Secrets? An Analysis of Procedural Rules and Technical Tools for the Protection of Trade Secrets in Arbitration in: Research Handbook on Intellectual Property Rights and Arbitration." Accessed July 29, 2025. https://www.elgaronline.com/edcollchap/book/9781800378360/book-part-9781800378360-15.xml.

"China's Personal Information Protection Law and Its Global Impact – The Diplomat." Accessed July 29, 2025. https://thediplomat.com/2021/08/chinas-personal-information-protection-law-and-its-global-impact/.

"Ciarb | Courses." Accessed July 29, 2025. https://www.ciarb.org/courses/.

"Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance | Interdisciplinary Studies in Society, Law, and Politics." Accessed July 29, 2025. http://193.36.85.187:8089/index.php/isslp/article/view/309.

Dincer, Yigit Efe. *Arbitration in the Age of Blockchain*. April 2024. http://hdl.handle.net/1866/33059.

"Evolving Paradigms of Trade Secret Protection: A Comparative Study of the US, EU, and India | Trends in Intellectual Property Research." Accessed July 29, 2025. https://iprtrends.com/TIPR/article/view/32.

Fortese, Fabricio, and Sophie Nappert. "Assessing Expert Evidence." SSRN Scholarly Paper No. 4976523. Social Science Research Network, April 1, 2025. https://papers.ssrn.com/abstract=4976523.

Ike, David. "PRESERVATION OF TRADE SECRETS PURSUANT TO TRIPS AGREEMENT AND EMERGING NATIONS." *Nnamdi Azikiwe University, Awka Journal of Public and Private Law* 11, no. 0 (2021): 0. https://ezenwaohaetorc.org/journals/index.php/UNIZIKJPPL/article/view/1670.

Junge, Fabian. "The Necessity of European Harmonization in the Area of Trade Secrets." SSRN Scholarly Paper No. 2839693. Social Science Research Network, September 16, 2016. https://doi.org/10.2139/ssrn.2839693.

Kaufmann-Kohler, Gabrielle, and Michele Potestà. *Investor-State Dispute Settlement and National Courts: Current Framework and Reform Options*. European Yearbook of International Economic Law. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-44164-7.

"LCIA Arbitration Rules 2020." Accessed July 29, 2025. https://www.lcia.org/Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx.

Millard, Christopher, and Christopher Millard, eds. *Cloud Computing Law*. Second Edition, Second Edition. Oxford University Press, 2021.

OECD. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." February 11, 2002. https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.

Shirlow, Esmé. "Transparency in Investment Treaty Arbitration: Past, Present, and Future." *Journal of International Dispute Settlement* 16, no. 3 (2025): idaf019. https://doi.org/10.1093/jnlids/idaf019.

"SIAC Rules 2025 - Singapore International Arbitration Centre." Accessed July 29, 2025. https://siac.org.sg/siac-rules-2025.

Singh, Nandini. "Schrems II: Impact on International Exchange of Personal Data." *Indian Journal of Law and Legal Research* 5 Issue 1 (2023): 1.

Stelea, Nicoleta, and Gavrila Calefariu. "International Arbitration and GDPR Application." *Romanian Arbitration Journal / Revista Romana de Arbitraj* 18 (2024): 75.

Teramura, Nobumichi, and Leon Trakman. "Confidentiality and Privacy of Arbitration in the Digital Era: Pies in the Sky?" *Arbitration International* 40, no. 3 (2024): 277–306. https://doi.org/10.1093/arbint/aiae017.

"The 2020 Revisions to the IBA Rules of Evidence | International Bar Association." Accessed July 29, 2025. https://www.ibanet.org/2020-revisions-to-IBA-rules-of-evidence-neuhaus-voser.

"The ICCA Reports No. 6: ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration | ICCA." Accessed July 29, 2025. https://www.arbitration-icca.org/icca-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration.

Voss, W. Gregory. "Cross-Border Data Flows, the GDPR, and Data Governance." *Washington International Law Journal* 29 (2020 2019): 485.