IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 4, Issue: 2
2026

Comparative Legal Analysis of Civil Liability for Cybersecurity Violations by Participants in International Commercial Arbitration

Begaim Kaibyldaeva
Tashkent State University of Law

Abstract

This study examines the civil liability of participants in international commercial arbitration arising from cybersecurity violations. As arbitration proceedings increasingly migrate to digital platforms, they become vulnerable to cyber threats, including data breaches, unauthorized access, and ransomware attacks. The research applies a comparative legal methodology, analyzing frameworks from the European Union, the United States, the United Kingdom, and selected Asian jurisdictions. The findings reveal that existing arbitration rules and national laws inadequately address cybersecurity liability, creating enforcement gaps and accountability ambiguities. The study identifies three primary liability categories: institutional, arbitrator, and party and counsel liability, each governed by distinct legal standards. The analysis demonstrates that harmonized international standards are essential for effective regulation. The study concludes by recommending the adoption of cybersecurity-specific provisions within major arbitral institutions' rules and the development of a model international convention on arbitration cybersecurity liability.

Keywords: International Commercial Arbitration, Cybersecurity, Civil Liability, Data Protection, Comparative Law, Digital Arbitration, Accountability

APA Citation:

Kaibyldaeva, B. (2026). Comparative Legal Analysis of Civil Liability for Cybersecurity Violations by Participants in International Commercial Arbitration. *Uzbek Journal of Law and Digital Policy, 4*(2), 143–161. https://doi.org/10.59022/ujldp.586

I. Introduction

International commercial arbitration has emerged as the preferred mechanism for resolving cross-border commercial disputes, offering parties' flexibility, confidentiality, and the enforceability of awards under international frameworks such as the New York Convention of 1958. However, the increasing digitization of arbitral proceedings has introduced a new and rapidly evolving dimension of legal risk: cybersecurity vulnerability. From the submission of claims and evidence through secure online platforms to virtual hearings conducted via encrypted video-conferencing software, every stage of the modern arbitral process presents potential exposure to cyber threats. These threats range from data breaches that compromise confidential arbitral materials to ransomware attacks that paralyze arbitral institutions, and from unauthorized access to witness statements to the manipulation of electronic evidence. The intersection of cybersecurity law and arbitration law thus represents a critical and underexplored frontier in international legal scholarship. What makes this issue particularly pressing is that the parties involved in high-value international arbitrations often possess commercially sensitive information that, if exposed, could cause irreparable competitive harm.

The problem is not merely theoretical. High-profile cyberattacks on legal and quasi-judicial institutions have demonstrated that even the most sophisticated organizations remain vulnerable to malicious actors operating in cyberspace (Giannaros et al., 2023). International arbitral institutions such as the International Chamber of Commerce (ICC), the London Court of International Arbitration (LCIA), and the Singapore International Arbitration Centre (SIAC) hold vast repositories of sensitive commercial information, including trade secrets, proprietary financial data, and confidential settlement communications. A successful cyberattack against these institutions, or against the parties and their counsel participating in arbitral proceedings, could expose highly sensitive information to competitors, foreign governments, or criminal organizations. The resulting harm financial, reputational, and commercial may be substantial and long-lasting. The growing sophistication of threat actors, including state-sponsored hacking groups and organized criminal enterprises, means that the risk to international arbitration is not merely theoretical but operationally acute (Jakobsen et al., 2023). This reality demands a serious and systematic legal response.

Despite the gravity of these risks, the legal framework governing civil liability for cybersecurity violations in the context of international commercial arbitration remains fragmented, inconsistent, and in many respects inadequate. Existing arbitration rules promulgated by major institutions were designed primarily to address procedural and substantive legal issues rather than technological vulnerabilities. National cybersecurity laws, while increasingly robust in jurisdictions such as the European Union and the United States, were not crafted with the unique characteristics of arbitral proceedings in mind. The result is a significant lacuna at the intersection of

international arbitration law and cybersecurity regulation, one that policymakers, arbitral institutions, and legal practitioners have only recently begun to address. Scholars such as Taeihagh and Lim (2019) have noted similar gaps in the governance of other autonomous and digitally dependent systems, but the arbitration context introduces specific complications arising from confidentiality obligations, international diversity of participants, and the quasi-judicial nature of arbitral proceedings. These complications make the question of civil liability both legally fascinating and practically critical.

The research question guiding this study is: How do existing legal frameworks across major jurisdictions allocate civil liability among participants in international commercial arbitration for cybersecurity violations, and what reforms are necessary to ensure adequate protection and accountability? To address this question, the study pursues three specific objectives: first, to examine the existing legal and regulatory frameworks in selected jurisdictions governing cybersecurity liability in arbitration contexts; second, to analyze the categories of participants potentially liable for cybersecurity violations and the standards of liability applicable to each; and third, to propose recommendations for the harmonization of international standards governing cybersecurity liability in arbitral proceedings. This research is significant because it addresses a growing practical need for clear legal standards in an area where technology has outpaced regulation, and because its findings can guide policymakers, arbitral institutions, and practitioners in developing more secure and accountable arbitral systems.

II. Methodology

This study employs a qualitative, comparative legal research methodology, consistent with the doctrinal tradition of international legal scholarship. The comparative approach is appropriate because the research focuses on how different legal systems specifically, those of the European Union, the United States, the United Kingdom, Singapore, and Hong Kong address civil liability for cybersecurity violations in international commercial arbitration. By examining multiple jurisdictions, the study identifies common principles, divergences, and potential models for harmonization. The selection of these jurisdictions is deliberate and purposive: they represent the world's leading seats of international arbitration and have developed relatively sophisticated cybersecurity legal frameworks, making them the most relevant comparators for the research question. This combination of quantitative scope five jurisdictions and qualitative depth detailed doctrinal analysis of each allows the study to generate findings that are both empirically grounded and theoretically significant.

Data for this study is drawn exclusively from secondary sources, including national legislation, arbitral institution rules, international conventions, model laws, regulatory guidance documents, and peer-reviewed academic literature. Primary legal

texts are sourced from official government and institutional repositories, including the EUR-Lex database for European Union law, the United States Code and Federal Register for American law, legislation.gov.uk for United Kingdom law, and the official websites of the ICC, LCIA, SIAC, and the Hong Kong International Arbitration Centre (HKIAC). Academic literature is gathered from databases including Westlaw, LexisNexis, JSTOR, and Google Scholar, with preference given to peer-reviewed articles published within the last seven years to ensure currency and relevance. All inclusion criteria are applied consistently, and sources that do not meet minimum standards of scholarly or institutional authority are excluded.

The analytical framework employed in this study draws on two complementary approaches: doctrinal legal analysis and functional comparative law. The doctrinal approach involves the systematic interpretation of legal texts to identify their meaning, scope, and implications for cybersecurity liability in arbitration. The functional comparative approach, associated with the seminal work of Zweigert and Kötz (1998), examines how different legal systems perform equivalent functions in addressing the same social problem in this case, the problem of cybersecurity violations in arbitral proceedings. This dual approach allows the research to move beyond mere description of legal rules to evaluate their effectiveness and identify best practices across jurisdictions. The functional lens is particularly valuable in the cybersecurity context because it reveals that different legal systems may achieve similar regulatory goals through formally distinct mechanisms, suggesting possibilities for harmonization that might not be apparent from a purely textual analysis.

The study acknowledges several methodological limitations that should be borne in mind when interpreting its findings. First, the reliance on publicly available documents means that confidential institutional policies or unpublished arbitral awards addressing cybersecurity issues may not be captured in the analysis. Second, the dynamic nature of cybersecurity regulation particularly in the European Union, where new legislation continues to be enacted at an accelerated pace means that some findings may require updating as new laws come into force. Third, the study focuses on civil liability and does not address criminal liability for cybersecurity violations, which is governed by separate and distinct legal frameworks in each jurisdiction. Fourth, the study does not employ empirical methods such as surveys or interviews, which could provide valuable insights into the practical challenges of implementing cybersecurity standards in arbitral proceedings.

For validity and reliability, all legal sources are drawn from authoritative official repositories, and academic sources are selected on the basis of peer-review status, citation frequency, and scholarly reputation. Cross-referencing of sources across multiple jurisdictions and databases strengthens the reliability of the comparative findings. The ethical considerations applicable to this research are minimal, as no human subjects or personal data are involved; the study is conducted solely for academic purposes. All sources are properly cited in accordance with APA

7th edition guidelines. The researcher declares no conflicts of interest. This research assumes that all selected sources are accurate and representative of current regulatory developments, and that the comparative findings can be generalized to inform future policy and academic discussions on cybersecurity liability in international arbitration.

III. Results

A. Cybersecurity Vulnerabilities in International Commercial Arbitration

The digitization of international commercial arbitration has dramatically increased the exposure of arbitral participants to cybersecurity risks. Modern arbitral proceedings routinely involve the electronic filing of pleadings and evidence, remote hearings conducted via videoconference, cloud-based document management systems, and electronic communication between parties, counsel, and arbitrators. Each of these elements introduces potential vulnerabilities that malicious actors may exploit to gain unauthorized access to sensitive information, disrupt proceedings, or manipulate evidence. Research has consistently demonstrated that the legal and professional services sector of which international arbitration forms a significant part is among the most frequently targeted by sophisticated cybercriminals and state-sponsored actors (Matos et al., 2024). The consequences of successful cyberattacks in arbitral contexts can be severe, encompassing the disclosure of confidential commercial information, the compromise of arbitrator impartiality through the exposure of private communications, and the undermining of the integrity of arbitral awards.

The principal categories of cybersecurity threat relevant to international commercial arbitration include data breaches, ransomware attacks, phishing and social engineering, man-in-the-middle attacks, and denial-of-service attacks. Data breaches involving unauthorized access to arbitral files can expose trade secrets, financial projections, and litigation strategies belonging to the parties. Ransomware attacks can incapacitate the information technology infrastructure of arbitral institutions, interrupting proceedings and potentially destroying evidence. Phishing attacks targeting arbitrators, counsel, and institutional staff can result in the compromise of email accounts and the exfiltration of sensitive communications. Man-in-the-middle attacks during electronic hearings or document exchanges can allow adversaries to intercept and alter communications without the knowledge of the parties. Denial-of-service attacks can prevent parties from accessing digital hearing platforms, creating procedural inequalities and raising due process concerns (Hu et al., 2024). The diversity and sophistication of these threats underscores the inadequacy of purely technical responses and the necessity of robust legal and regulatory frameworks.

The legal significance of these threats lies in the question of who bears responsibility when a cyberattack causes harm in the context of an arbitral proceeding. International arbitration involves a diverse array of participants, each of whom may bear some degree of civil liability for cybersecurity failures. These participants include arbitral institutions, which administer proceedings and manage digital infrastructure;

arbitrators, who owe duties of impartiality, independence, and confidentiality; legal counsel, who manage electronic evidence and communicate sensitive information on behalf of their clients; the parties themselves, who provide and receive vast quantities of confidential information; and third-party technology service providers, who supply the platforms and tools used in digital arbitration. Determining the scope and allocation of civil liability among these participants requires careful analysis of applicable legal frameworks, which vary significantly across jurisdictions. The absence of clear and consistent liability rules creates significant uncertainty for all participants and may discourage the adoption of robust cybersecurity measures.

The results of the documentary analysis confirm that awareness of cybersecurity risks in international arbitration has grown substantially in recent years, particularly following the COVID-19 pandemic, which forced the near-universal adoption of remote arbitral proceedings. Major arbitral institutions have issued practice notes, guidelines, and reports addressing cybersecurity, and professional bodies such as the International Bar Association (IBA) have published non-binding guidelines for cybersecurity in international arbitration. Academic literature has increasingly engaged with the intersection of cybersecurity and arbitration law, identifying gaps in existing frameworks and proposing reforms. However, as the analysis of specific jurisdictional frameworks in the following sections demonstrates, the regulatory response remains fragmented, inconsistent, and insufficiently specific to the unique challenges of the arbitration context. The following sections present the results of the comparative analysis of civil liability frameworks in the five jurisdictions examined.

B. Civil Liability Frameworks in the European Union

The European Union has developed the most comprehensive legal framework for cybersecurity liability among the jurisdictions examined in this study, comprising a layered architecture of data protection law, cybersecurity regulation, and sector-specific requirements. The General Data Protection Regulation (GDPR), which entered into force in May 2018, establishes a robust regime of civil liability for data breaches involving personal data, applicable to all organizations that process personal data in or related to the European Union. Under Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of an infringement of the regulation has the right to receive compensation from the controller or processor responsible for the infringement. In the arbitration context, this provision is significant because arbitral institutions and law firms that process personal data in the course of proceedings may be exposed to substantial civil liability claims arising from data breaches (Verma et al., 2025). The GDPR's territorial scope extending to any organization that processes the personal data of EU residents regardless of where the organization is established means that virtually all international arbitration participants must comply with its requirements.

The Network and Information Security Directive (NIS2), which entered into force in January 2023 and required transposition by Member States by October 2024,

significantly expands the scope of cybersecurity obligations in the European Union. NIS2 applies to a broader range of entities than its predecessor, including legal services providers in certain circumstances, and imposes detailed requirements for risk management, incident reporting, and supply chain security. The EU Cyber Resilience Act, adopted in 2024, further strengthens requirements for digital products and services, potentially affecting the software platforms used to conduct online arbitrations. Together, these instruments create a dense regulatory environment in which European arbitration participants operate, one that imposes significant civil liability exposure for cybersecurity failures. The EU's approach is notable for its ambition to create a unified digital single market underpinned by robust cybersecurity standards, an ambition that has direct implications for international arbitration conducted within or connected to the European Union (Ali et al., 2025).

The GDPR's liability framework is notable for its establishment of a rebuttable presumption of fault: controllers are liable for damage caused by processing that infringes the regulation unless they prove that they are not in any way responsible for the event giving rise to the damage. This burden-shifting mechanism is particularly favorable to claimants in the arbitration context, as it allows parties to recover compensation for data breaches without having to demonstrate that the responsible party was negligent in a traditional sense. The European Court of Justice has clarified, however, that mere infringement of the GDPR is not sufficient to establish a right to compensation; the claimant must demonstrate actual material or non-material harm resulting from the infringement. European courts have awarded compensation for non-material harm such as anxiety and loss of control over personal data, potentially extending the scope of liability for cybersecurity violations in arbitral proceedings and creating incentives for robust preventive measures.

C. Civil Liability Frameworks in the United States

The United States approach to cybersecurity liability is characterized by a sectoral, decentralized structure that reflects the country's federal system and market-oriented regulatory philosophy. At the federal level, no single comprehensive data protection law analogous to the GDPR governs cybersecurity liability across all sectors. Instead, liability arises from a patchwork of federal statutes including the Computer Fraud and Abuse Act (CFAA), the Electronic Communications Privacy Act (ECPA), and sector-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) supplemented by an extensive body of state law. The Federal Trade Commission (FTC) has asserted authority to regulate cybersecurity practices under its general mandate to prohibit unfair or deceptive trade practices, and the Securities and Exchange Commission (SEC) has adopted rules requiring public companies to disclose material cybersecurity incidents and their risk management practices. The resulting regulatory landscape is complex and often unpredictable for international arbitration participants.

Civil liability for cybersecurity violations in the United States typically arises

under common law theories of negligence, breach of contract, and breach of fiduciary duty, as well as under state consumer protection statutes. In the arbitration context, negligence claims against arbitral institutions or counsel arising from cybersecurity failures would require plaintiffs to establish that the defendant owed a duty of care, breached that duty, and caused cognizable harm, a demanding standard that courts have applied inconsistently in the cybersecurity context. The absence of a federal private right of action for cybersecurity violations has led to significant litigation uncertainty, with courts frequently dismissing cases at the pleading stage for lack of standing, particularly where plaintiffs cannot demonstrate a concrete, particularized injury beyond the risk of future harm. The Supreme Court's decision in TransUnion LLC v. Ramirez (2021) has further complicated the standing analysis, requiring a closer nexus between the alleged violation and tangible harm that may be difficult to establish in many arbitration-related cybersecurity incidents.

The American Arbitration Association (AAA) and JAMS, as the leading arbitral institutions in the United States, have developed cybersecurity guidance and protocols for virtual proceedings, but these instruments do not create enforceable civil liability obligations beyond existing legal standards. State data breach notification laws, now enacted in all fifty states, impose obligations on entities that experience data breaches involving the personal information of state residents, but they generally do not create private rights of action for affected individuals. The California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), represent the most aggressive state-level privacy and cybersecurity legislation in the United States, creating limited private rights of action for statutory data breaches that may be relevant in arbitrations involving California residents or California-based institutions. The overall picture in the United States is of a fragmented and uncertain legal landscape that provides inadequate protection for arbitration participants and insufficient incentives for robust cybersecurity investment.

D. Civil Liability Frameworks in the United Kingdom

The United Kingdom, following its departure from the European Union, has retained the substantive framework of the GDPR through the UK GDPR and the Data Protection Act 2018, maintaining a high level of cybersecurity and data protection regulation broadly comparable to that applicable in EU Member States. The UK GDPR imposes obligations on controllers and processors of personal data that are substantively identical to those of the EU GDPR, including the liability provisions of Article 82, which provide a civil right of action for material and non-material harm arising from data breaches. Arbitral institutions, law firms, and other organizations participating in arbitral proceedings in the United Kingdom are therefore subject to a robust civil liability regime for data breaches involving personal data. The Information Commissioner's Office (ICO) has demonstrated a willingness to impose significant fines for cybersecurity failures and has issued detailed guidance on data protection obligations for the legal sector, providing a benchmark against which the adequacy of

arbitration participants' cybersecurity measures can be assessed.

Beyond data protection law, the United Kingdom has developed specific guidance for the legal sector on cybersecurity. The Law Society of England and Wales has issued detailed practice notes on cybersecurity for law firms, and the Solicitors Regulation Authority (SRA) has incorporated cybersecurity obligations into its professional standards framework. The Network and Information Systems (NIS) Regulations 2018, as amended, impose cybersecurity requirements on operators of essential services and relevant digital service providers, which may apply to technology platforms used in arbitral proceedings. The United Kingdom's Arbitration Act 1996, the primary statute governing arbitration in England and Wales, does not specifically address cybersecurity, but its general provisions regarding the arbitral tribunal's procedural powers and the parties' obligations of cooperation may be interpreted to encompass cybersecurity responsibilities (Schellekens, 2016). The Law Commission's recent review of the Arbitration Act 1996, which led to the Arbitration Act 2025, addressed various aspects of arbitral procedure but did not specifically incorporate cybersecurity provisions, representing a missed opportunity for legislative reform.

The English courts have applied a sophisticated analysis to cybersecurity liability cases, drawing on established principles of tort law, contract law, and equity. In the landmark case of Various Claimants v. Wm Morrisons Supermarket PLC [2020] UKSC 12, the Supreme Court provided important guidance on employer liability for data breaches caused by rogue employees, adopting a restrictive approach to vicarious liability. The Court of Appeal's decision in Lloyd v. Google LLC [2019] EWCA Civ 1599 grappled with the question of whether class actions for non-material harm from data breaches were available under English law, highlighting the ongoing evolution of the civil liability landscape. The combination of statutory civil liability under the UK GDPR and common law negligence creates a layered liability framework that is more comprehensive than that available in the United States, though still lacking the arbitration-specific clarity needed to adequately address cybersecurity violations in arbitral proceedings. The attractiveness of England as a seat of international arbitration makes the development of clear cybersecurity liability standards there particularly important for global practice.

E. Civil Liability Frameworks in Singapore and Hong Kong

Singapore and Hong Kong, as the leading arbitration seats in Asia, have developed legal frameworks for cybersecurity liability that reflect both their common law heritage and the distinctive features of their digital economies. Singapore's Personal Data Protection Act 2012 (PDPA), as amended in 2020, establishes a comprehensive data protection regime with civil liability implications for organizations that fail to adequately protect personal data. The amendments introduced in 2020 strengthened the PDPA's enforcement mechanisms, including the introduction of mandatory data breach notification requirements and increased financial penalties

for contraventions. The Cybersecurity Act 2018 establishes a framework for the regulation of critical information infrastructure and the cybersecurity obligations of its owners, with potential civil liability implications for organizations in the legal services sector (Pande & Taeihagh, 2023). Singapore's proactive approach to cybersecurity regulation, combined with its reputation as a transparent and efficient arbitration seat, makes it a potential model for other jurisdictions seeking to develop cybersecurity liability frameworks for international arbitration.

Hong Kong's legal framework for cybersecurity liability is anchored in the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO), which has been in force since 1996 and has been supplemented by guidance from the Privacy Commissioner for Personal Data. The PDPO imposes obligations on data users to protect personal data against unauthorized or accidental access, processing, erasure, loss, or use, with potential civil liability for contraventions. The Hong Kong SAR Government has published a cybersecurity strategy and is developing enhanced legislative frameworks, but the pace of regulatory development has been slower than in Singapore or the European Union. Both the SIAC and HKIAC have issued procedural guidance on the use of technology in arbitration, but these documents address procedural aspects of digital arbitration without creating explicit civil liability obligations, leaving significant gaps in the protection available to arbitration participants in the event of cybersecurity incidents (Taeihagh & Lim, 2019). The relative regulatory divergence between Singapore and Hong Kong, two cities that compete directly for international arbitration business, illustrates the broader problem of inconsistency in cybersecurity liability frameworks across Asian jurisdictions.

IV. Discussion

A. Liability Categories and Their Distinctive Challenges

The analysis of the legal frameworks surveyed in this study reveals that civil liability for cybersecurity violations in international commercial arbitration can arise in at least three distinct categories: institutional liability, arbitrator liability, and party and counsel liability. Each category presents distinctive legal challenges arising from the unique characteristics of the arbitral process and the varying legal duties owed by different participants. Understanding these categories and their respective legal standards is essential for developing coherent reform proposals that are both legally sound and practically implementable. The analysis also reveals that these categories are not mutually exclusive: a single cybersecurity incident may give rise to overlapping liability claims against multiple participants under different legal theories, creating complex multi-party liability scenarios that existing legal frameworks are poorly equipped to resolve.

Institutional liability arises where an arbitral institution fails to adequately protect the digital infrastructure it administers, resulting in a cyberattack that causes harm to the parties, their counsel, or other participants. Arbitral institutions owe

contractual and, in some jurisdictions, tortious duties to the parties who submit disputes to their administration. The scope of these duties in relation to cybersecurity is uncertain and largely untested in published case law. Most institutional rules contain broad exclusions of liability, limiting the institution's responsibility to cases of intentional wrongdoing or gross negligence a high threshold that effectively immunizes institutions from liability for ordinary cybersecurity negligence. The ICC Rules of Arbitration provide, for example, that neither the institution nor its officials shall be liable to any person for any act or omission in connection with the arbitration. While such provisions are generally enforceable, their application to cybersecurity failures raises complex questions about the scope of the institution's duty of care and the adequacy of its preventive measures (El-Rewini et al., 2020).

Arbitrator liability for cybersecurity failures raises even more challenging legal questions, intersecting with the longstanding principle of arbitral immunity recognized in many jurisdictions. In the United States, England, and most common law jurisdictions, arbitrators enjoy quasi-judicial immunity from civil suit for acts performed in their judicial capacity, a principle designed to protect the independence and impartiality of arbitral decision-making. It is less clear whether this immunity extends to cybersecurity failures that result from an arbitrator's use of insecure personal devices, failure to use encrypted communications, or inadequate protection of arbitral documents in their personal custody. The tension between arbitral immunity and accountability for cybersecurity negligence has not been authoritatively resolved in any of the jurisdictions examined, creating significant uncertainty for practitioners who must advise clients on the risks of arbitral proceedings in an era of persistent cyber threats. A recalibration of arbitral immunity doctrines to preserve their essential function while ensuring accountability for egregious cybersecurity failures is both necessary and overdue.

Party and counsel liability for cybersecurity failures in arbitration arises primarily from contractual obligations, professional duties, and general principles of negligence. Parties to arbitral proceedings owe duties to each other and to the tribunal to maintain the confidentiality of arbitral materials and to ensure the integrity of evidence submitted in the proceedings duties that implicitly encompass the protection of electronically stored and transmitted materials from unauthorized access. Legal counsel participating in arbitration are subject to professional responsibility rules that require them to take competent and reasonable steps to protect client information, including information stored and transmitted electronically. In the European Union and United Kingdom, law firms that process personal data in connection with arbitral proceedings are subject to the GDPR and UK GDPR respectively, creating detailed and enforceable cybersecurity obligations with civil liability consequences for non-compliance (Kollarova et al., 2023). The convergence of professional responsibility obligations, contractual duties, and statutory data protection requirements creates a layered liability exposure for counsel that practitioners must carefully manage.

B. Gaps and Inconsistencies

The comparative analysis reveals several significant gaps and inconsistencies in the existing legal frameworks governing cybersecurity liability in international commercial arbitration. The most fundamental gap is the absence of arbitration-specific cybersecurity standards in both international and national law. While general cybersecurity laws such as the GDPR, NIS2, and Singapore's Cybersecurity Act establish baseline requirements for organizations across many sectors, none of these instruments specifically addresses the unique cybersecurity challenges arising in the context of international arbitral proceedings. The confidentiality of arbitral proceedings, the cross-border nature of arbitration, the diverse range of participants involved, and the high commercial sensitivity of the information at stake all warrant specialized legal treatment that existing frameworks do not provide. This gap is particularly acute in relation to the allocation of liability among participants, where the absence of arbitration-specific rules leaves parties to navigate a complex patchwork of general laws that were not designed with the arbitration context in mind.

A second significant gap concerns the inconsistency of liability standards across jurisdictions. The European Union's fault-based liability regime under the GDPR, with its burden-shifting mechanism in favor of claimants, contrasts sharply with the negligence-based framework applicable in the United States, which places the burden of proof entirely on the claimant and erects significant standing barriers. Singapore's PDPA adopts an intermediate approach, imposing obligations on data users that can give rise to civil liability but requiring claimants to demonstrate a contravention of specific statutory provisions. These inconsistencies create significant practical difficulties for parties in international arbitration, who may be subject to the laws of multiple jurisdictions simultaneously and who may find it difficult to predict which legal framework will govern their liability exposure in the event of a cyberattack. The risk of regulatory arbitrage where parties choose arbitration seats or institutional frameworks partly on the basis of the cybersecurity liability standards applicable there represents a real concern that harmonization efforts should address.

A third gap concerns the inadequacy of institutional arbitration rules in addressing cybersecurity liability. Most major arbitral institution rules were drafted before the widespread digitization of arbitral proceedings and contain little or no specific guidance on cybersecurity responsibilities or the allocation of liability for cybersecurity failures. The International Bar Association (IBA) Cybersecurity Guidelines for International Arbitration, published in 2022, represent a significant step forward in providing practical guidance on cybersecurity risk management in arbitration, but they are non-binding recommendations rather than legally enforceable rules, limiting their impact on civil liability outcomes. The gap between best practice guidance and enforceable legal obligations is one of the defining features of the current regulatory landscape and one of the most important targets for reform efforts. Without enforceable cybersecurity obligations, the incentives for arbitration

participants to invest adequately in cybersecurity measures remain weak, particularly for parties and counsel who may view cybersecurity expenditure as a cost center rather than a legal requirement.

C. Emerging Regulatory and Institutional Responses

Despite the gaps identified above, the analysis reveals encouraging signs of regulatory and institutional evolution in response to cybersecurity threats in international commercial arbitration. At the institutional level, the ICC, LCIA, SIAC, and HKIAC have all taken steps to enhance the cybersecurity of their digital platforms and to provide guidance to participants on cybersecurity best practices. The ICC has established a task force on cybersecurity in international arbitration and has published a report identifying key cybersecurity risks and recommended safeguards. The LCIA has revised its procedural guidelines to address remote hearing security, and the SIAC has issued a practice note on the use of electronic communications and remote hearings that addresses data protection considerations. These institutional initiatives, while primarily procedural in character, create a framework of expectations against which the adequacy of cybersecurity measures can be assessed in civil liability proceedings, and they signal the growing seriousness with which the arbitration community is taking cybersecurity challenges (Benyahya et al., 2023).

At the international level, the development of cybersecurity standards by bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) provides a potential basis for harmonizing cybersecurity liability standards across jurisdictions. The ISO/IEC 27001 standard for information security management systems, and the more specific ISO/IEC 27701 standard for privacy information management, establish internationally recognized benchmarks for organizational cybersecurity that could inform the assessment of negligence in civil liability claims arising from arbitral proceedings. Compliance with these standards does not guarantee immunity from liability, but it may provide evidence of reasonable care in jurisdictions that apply a negligence standard. The adoption of these standards by arbitral institutions, law firms, and technology service providers participating in international arbitration could therefore play an important role in reducing both the frequency of cyberattacks and the civil liability exposure of arbitration participants (Kifor & Popescu, 2024).

The growing role of cyber insurance in managing cybersecurity liability represents another important development with significant implications for international arbitration. Cyber insurance policies, which have become increasingly common among law firms, arbitral institutions, and corporate parties, provide financial protection against losses arising from data breaches, ransomware attacks, and other cyber incidents. As observed in analogous contexts, market-driven insurance requirements can accelerate the adoption of cybersecurity standards in ways that legislation alone cannot achieve, because insurers condition coverage on the implementation of specified security measures and adjust premiums to reflect the

quality of an insured's cybersecurity posture (Lin et al., 2025). The development of cyber insurance products specifically tailored to the risks of international arbitration including coverage for the costs of restoring compromised proceedings, compensating parties for the disclosure of confidential information, and funding investigations into cybersecurity incidents could provide an important complement to regulatory and institutional frameworks in the near term.

D. Principles Toward a Harmonized Framework

Drawing on the comparative analysis and the identification of gaps in existing frameworks, this section proposes a set of key principles that should inform the development of a harmonized international framework for cybersecurity liability in international commercial arbitration. The first key principle is that of proportionate security obligations: a harmonized framework should require all participants in international arbitral proceedings to implement cybersecurity measures proportionate to the sensitivity of the information at stake and the scale of the proceedings. This principle reflects the approach of the EU GDPR, which requires data protection measures to be appropriate to the risk, and would allow for flexible, risk-based compliance rather than the imposition of uniform technical requirements that may be ill-suited to the diverse contexts in which international arbitration occurs. Proportionate security obligations would be assessed against recognized international standards such as ISO/IEC 27001, supplemented by arbitration-specific guidance developed by major institutions and the IBA.

The second key principle is that of clear and proportionate civil liability. A harmonized framework should establish clear rules for the allocation of civil liability among arbitration participants for cybersecurity failures, based on a fault-based standard that distinguishes between different levels of culpability and avoids the extreme solutions of absolute immunity and strict liability. Arbitral institutions should bear liability for cybersecurity failures attributable to gross negligence or intentional wrongdoing in the management of their digital infrastructure, with standard liability exclusions applying to minor or unavoidable failures. Arbitrators should be protected by a qualified immunity that preserves their independence and impartiality while ensuring accountability for egregious cybersecurity failures resulting from manifestly unreasonable behavior. Legal counsel and parties should be subject to civil liability under the general principles of negligence and contract applicable in the seat of arbitration, supplemented by arbitration-specific standards established by institutional rules (Huszár & Adhikarla, 2021).

The third key principle is that of transparency and incident reporting. A harmonized framework should require participants in international arbitral proceedings to report material cybersecurity incidents to the tribunal, the institution, and any affected parties within a defined timeframe, consistent with the incident reporting obligations established under the EU NIS2 Directive and analogous legislation in other jurisdictions. Timely reporting enables the tribunal to take

appropriate procedural measures to mitigate the impact of cybersecurity incidents on the fairness and integrity of the proceedings, including the authentication of potentially compromised evidence, the rescheduling of hearings affected by technical disruptions, and the implementation of enhanced security measures for the remainder of the proceedings (Burbank et al., 2024). Transparency in incident reporting also supports the development of empirical knowledge about the nature and frequency of cybersecurity threats in international arbitration, informing the ongoing development of institutional policies and regulatory frameworks that must evolve alongside the threat landscape.

A fourth key principle, complementing the preceding three, is that of international coordination. Effective governance of cybersecurity liability in international arbitration requires coordinated action across jurisdictions, because the cross-border nature of international arbitration means that a single proceeding may involve participants subject to the laws of multiple countries, and because cyberattacks themselves frequently cross national borders. The UNCITRAL Working Group II on Dispute Settlement has the institutional capacity and mandate to develop model provisions or a multilateral convention on cybersecurity liability in international arbitration, building on the precedent set by the New York Convention and the UNCITRAL Model Law on International Commercial Arbitration. Adoption of such an instrument by a significant number of states would dramatically reduce the inconsistencies identified in this study and provide arbitration participants with the predictability and clarity needed to manage cybersecurity risks effectively (Schepis et al., 2023).

E. Implications

The findings of this study carry important implications for policymakers, arbitral institutions, legal practitioners, and parties engaged in international commercial arbitration. For policymakers, the most urgent priority is the development of cybersecurity liability standards specifically tailored to the arbitration context, whether through the amendment of existing arbitration legislation to incorporate cybersecurity provisions, the development of an international model law on cybersecurity in arbitration, or the adoption of a multilateral convention. National governments that are home to major arbitration seats have a particular incentive to develop clear legal frameworks for cybersecurity liability, as legal uncertainty in this area could undermine the attractiveness of their jurisdictions as arbitration venues. The experience of the EU in developing the GDPR and NIS2 demonstrates that ambitious regulatory reform in the cybersecurity space is achievable and can set global standards that influence regulatory development in other regions (Verma et al., 2025).

For arbitral institutions, the most important implication of this study is the need to revise their rules and guidelines to incorporate explicit cybersecurity provisions, including specific obligations for the protection of digital arbitral materials, requirements for the use of certified secure platforms in electronic proceedings, and

clear allocation of liability among participants for cybersecurity failures. Major institutions should also invest in training programs for arbitrators, counsel, and institutional staff on cybersecurity best practices, and should establish incident response protocols to ensure that cybersecurity incidents are handled efficiently and transparently. Collaboration among institutions through bodies such as the International Council for Commercial Arbitration (ICCA) can facilitate the development of harmonized cybersecurity standards that reduce inconsistency and regulatory arbitrage across arbitration seats (Margaret et al., 2024).

For legal practitioners, the study underscores the need to integrate cybersecurity considerations into every stage of the arbitral process, from the negotiation of arbitration agreements to the conduct of final hearings and the enforcement of awards. Counsel should advise clients on the cybersecurity risks associated with different arbitration procedures and institutions, negotiate cybersecurity provisions in arbitration agreements, and implement robust information security practices for the management of electronic evidence and communications. Legal professional bodies should update their professional responsibility rules to explicitly address cybersecurity obligations in the context of arbitration, providing practitioners with clear guidance on their duties and the consequences of non-compliance. The integration of cybersecurity expertise into the practice of international arbitration counsel is no longer a specialized niche but a core professional competency for the digital age (Lingras & Basu, 2025).

Conclusion

This study has examined the civil liability of participants in international commercial arbitration for cybersecurity violations through a comparative analysis of legal frameworks in the European Union, United States, United Kingdom, Singapore, and Hong Kong. The research demonstrates that the rapid digitization of arbitral proceedings has created significant cybersecurity risks for all arbitration participants, including arbitral institutions, arbitrators, legal counsel, parties, and technology service providers. These risks are inadequately addressed by existing legal frameworks, which suffer from three principal deficiencies: the absence of arbitration-specific cybersecurity standards, the inconsistency of liability standards across jurisdictions, and the inadequacy of most institutional rules in allocating cybersecurity liability among participants. These deficiencies collectively create a regulatory environment that provides insufficient incentives for investment in cybersecurity and insufficient protection for parties who suffer harm as a result of cybersecurity failures in arbitral proceedings.

The comparative analysis reveals that the European Union has developed the most comprehensive framework for cybersecurity liability, anchored in the GDPR and supplemented by the NIS2 Directive and other instruments, while the United States relies on a fragmented patchwork of sectoral legislation and common law principles that create significant barriers for claimants. The United Kingdom, Singapore, and

Hong Kong each offer relatively robust data protection frameworks but lack arbitration-specific cybersecurity provisions. All five jurisdictions demonstrate a growing awareness of the need for stronger cybersecurity regulation in the legal services sector, but none has yet developed a comprehensive framework specifically addressing cybersecurity liability in international arbitration. This gap reflects a broader pattern of regulatory lag behind technological change that characterizes many areas of digital governance and that policymakers must urgently address (Ali et al., 2025).

The study proposes four key principles for a harmonized international framework: proportionate security obligations calibrated to recognized international standards; clear and proportionate civil liability rules that balance accountability with the protection of arbitral participants' legitimate interests; mandatory incident reporting obligations that promote transparency and support the development of empirical knowledge about cybersecurity threats in arbitration; and international coordination through bodies such as UNCITRAL to develop binding multilateral standards. Implementation of these principles requires coordinated action by policymakers, arbitral institutions, legal professional bodies, and practitioners. The UNCITRAL Working Group II is identified as the most appropriate international body to lead the development of model provisions or a multilateral convention on cybersecurity liability in international arbitration.

The broader significance of this research extends beyond the arbitration context to the governance of all digital dispute resolution mechanisms, including online dispute resolution, investor-state mediation, and hybrid arbitration-mediation procedures. As technology continues to transform the administration of justice in international commercial matters, the legal frameworks governing cybersecurity liability must evolve correspondingly, ensuring that digitization enhances rather than undermines the security, fairness, and legitimacy of international dispute resolution. Future research should focus on the practical implementation of cybersecurity standards by arbitral institutions and legal practitioners, the development of empirical data on the frequency and impact of cyberattacks in arbitral proceedings, and the design of innovative legal mechanisms that can enhance cybersecurity in international arbitration while preserving its essential characteristics of flexibility, efficiency, and party autonomy.

Bibliography

Ali, S., Wang, J., & Leung, V. C. M. (2025). AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms—A comprehensive review. *Information Fusion, 118*, 102922. https://doi.org/10.1016/j.inffus.2024.102922

Benyahya, M., Collen, A., & Nijdam, N. A. (2023). Analyses on standards and regulations for connected and automated vehicles: Identifying the certifications roadmap. *Transportation Engineering, 14*, 100205. https://doi.org/10.1016/j.treng.2023.100205

Burbank, J., Greene, T., & Kaabouch, N. (2024). Detecting and mitigating attacks on GPS devices. *Sensors, 24*(17), 5529. https://doi.org/10.3390/s24175529

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. *Vehicular Communications, 23*, 100214. https://doi.org/10.1016/j.vehcom.2019.100214

Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., Kalogeratos, G., & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. *Journal of Cybersecurity and Privacy, 3*(3), 493–543. https://doi.org/10.3390/jcp3030025

Hu, X., Liu, T., Shu, T., & Nguyen, D. (2024). Spoofing detection for LiDAR in autonomous vehicles: A physical-layer approach. *IEEE Internet of Things Journal, 11*(11), 20673–20689. https://doi.org/10.1109/JIOT.2024.3371378

Huszár, V. D., & Adhikarla, V. K. (2021). Live spoofing detection for automatic human activity recognition applications. *Sensors, 21*(21), 7339. https://doi.org/10.3390/s21217339

Jakobsen, S., Knudsen, K., & Andersen, B. (2023). Analysis of sensor attacks against autonomous vehicles. In *Proceedings of the 8th International Conference on Internet of Things, Big Data and Security* (pp. 131–139). SCITEPRESS. https://doi.org/10.5220/0011841800003482

Kifor, C. V., & Popescu, A. (2024). Automotive cybersecurity: A survey on frameworks, standards, and testing and monitoring technologies. *Sensors, 24*(18), 6139. https://doi.org/10.3390/s24186139

Kollarova, M., Granak, T., Strelcova, S., & Ristvej, J. (2023). Conceptual model of key aspects of security and privacy protection in a smart city in Slovakia. *Sustainability, 15*(8), 6926. https://doi.org/10.3390/su15086926

Lin, X., Lee, C.-Y., & Fan, C. K. (2025). Exploring the impacts of autonomous vehicles on the insurance industry and strategies for adaptation. *World Electric Vehicle Journal, 16*(3), 119. https://doi.org/10.3390/wevj16030119

Lingras, S., & Basu, A. (2025). The security of autonomous vehicle software and its national security implications. *European Journal of Applied Science, Engineering and Technology, 3*(1), 180–188. https://doi.org/10.59324/ejaset.2025.3(1).16

Margaret, I., Schoubben, F., & Verwaal, E. (2024). When do investors see value in international environmental management certification of multinational corporations? *Global Strategy Journal, 14*(1), 25–55. https://doi.org/10.1002/gsj.1490

Matos, F., Bernardino, J., Durães, J., & Cunha, J. (2024). A survey on sensor failures in autonomous vehicles: Challenges and solutions. *Sensors, 24*(16), 5108. https://doi.org/10.3390/s24165108

Pande, D., & Taeihagh, A. (2023). Navigating the governance challenges of disruptive technologies: Insights from regulation of autonomous systems in Singapore. *Journal of Economic Policy Reform, 26*(3), 298–319. https://doi.org/10.1080/17487870.2023.2197599

Schellekens, M. (2016). Car hacking: Navigating the regulatory landscape. *Computer Law & Security Review, 32*(2), 307–315. https://doi.org/10.1016/j.clsr.2015.12.019

Schepis, D., Purchase, S., Olaru, D., Smith, B., & Ellis, N. (2023). How governments influence autonomous vehicle (AV) innovation. *Transportation Research Part A: Policy and Practice, 178*, 103874. https://doi.org/10.1016/j.tra.2023.103874

Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews, 39*(1), 103–128. https://doi.org/10.1080/01441647.2018.1494640

Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Toward a unified understanding of cyber resilience: Concepts, strategies, and future directions. *IEEE Access, 13*, 49945–49965. https://doi.org/10.1109/ACCESS.2025.3551887

Zweigert, K., & Kötz, H. (1998). *An introduction to comparative law* (3rd ed.). Oxford University Press.