

ALLOCATION OF CYBER RISK BETWEEN ARBITRAL INSTITUTIONS AND PARTIES UNDER UZBEK CIVIL LAW: TOWARDS A STATUTORY FRAMEWORK

Kaibylidaeva Begaim Mukhitovna

Independent Researcher,

Tashkent State University of Law

E-mail: begaimkaibylidaeva@gmail.com

<https://doi.org/10.5281/zenodo.21064931>

Introduction. The increasing reliance of international commercial arbitration on digital infrastructure has created a new and largely unresolved category of legal risk: the cyber incident that disrupts, compromises, or destroys data held by an arbitral institution or by the parties themselves. When a ransomware attack encrypts an institution's case-management platform, when a state-sponsored intrusion exfiltrates confidential pleadings, or when a party's own systems are breached and evidence is altered, the question of who bears the resulting financial and procedural loss becomes acute. Yet no jurisdiction has enacted legislation that directly addresses the allocation of cyber risk in the arbitral context, and Uzbekistan is no exception.¹

This article examines how the existing Uzbek civil-law framework, centred on the Civil Code of the Republic of Uzbekistan and the sector-specific legislation on cybersecurity and electronic documents, interacts with the rules of the Tashkent International Arbitration Centre (TIAC) to distribute cyber risk between institutions and parties. It argues that the current framework, while not wholly inadequate, contains significant gaps that expose both institutions and parties to unpredictable liability and that a targeted statutory amendment is needed to provide certainty.

The analysis proceeds in four stages: first, a mapping of the applicable civil-law principles; second, an examination of the cybersecurity obligations imposed on institutions and parties by public law; third, an identification of the allocative gaps; and fourth, the outlines of a proposed statutory framework.

Civil-Law Foundations for Cyber-Risk Allocation. The primary instrument of Uzbek private law is the Civil Code of the Republic of Uzbekistan. Part One, approved by Law No. 163-I of 21 December 1995, and Part Two, approved by Law No. 256-I of 29 August 1996 (both as amended to date), together govern the law of obligations, contractual liability, and extra-contractual harm.²

Article 333 of the Civil Code establishes the fault-based general rule: a debtor is liable for non-performance or improper performance of an obligation where fault is present, unless the law or the contract provides otherwise. This default rule has direct relevance in the arbitral context: where an institution undertakes, expressly or by implication, to maintain the confidentiality and integrity of the case file, a breach of that undertaking caused by a foreseeable cyber incident that the institution failed to prevent may give rise to contractual

¹ Born, G. B. (2021). *International Commercial Arbitration* (3rd ed.). Kluwer Law International. (On institutional liability and cyber risk in arbitration.)

² Civil Code of the Republic of Uzbekistan, Part One (Law No. 163-I, 21 December 1995); Part Two (Law No. 256-I, 29 August 1996). <https://lex.uz/docs/111181>

liability under Article 324 (the obligation to compensate losses arising from breach). The measure of those losses is the actual damage and lost profit established under Article 14.³

Extra-contractual liability is governed by Chapter 59 of Part Two of the Civil Code (Articles 985-1022). Article 985 provides that damage caused to the person or property of a citizen, or to the property of a legal entity, shall be compensated in full by the person who caused the harm. Article 986 creates a presumption of fault, placing on the tortfeasor the burden of proving absence of fault. For cyber incidents, this means that a party whose inadequately secured systems transmit malware to an institution's network, or an institution whose negligent configuration allows exfiltration of a party's confidential submissions, faces a *prima facie* liability claim under these provisions. Critically, Article 1000 imposes strict liability for harm caused by sources of increased danger, and there is a credible argument, not yet resolved in Uzbek case law, that large-scale digital infrastructure qualifies as such a source.⁴

Force majeure is addressed in Article 337 of the Civil Code, which excuses a debtor's non-performance where it results from circumstances of irresistible force (force majeure): extraordinary and unavoidable circumstances. A sophisticated targeted cyber attack by a state-level threat actor may qualify; a generic ransomware infection of unpatched systems almost certainly will not, given that the vulnerability would have been foreseeable and preventable. The burden of proving the force-majeure character of the incident lies on the party invoking it, and institutions should not assume that labelling an incident a "cyber attack" is sufficient to engage this defence.⁵

Public-Law Cybersecurity Obligations and Their Civil-Law Consequences. The Law of the Republic of Uzbekistan "On Cybersecurity" No. ZRU-764 of 15 April 2022 (entered into force 17 July 2022; adopted by the Legislative Chamber on 25 February 2022 and approved by the Senate on 17 March 2022) establishes a mandatory duty of care for entities operating information systems. Article 14 requires state bodies and organisations to ensure cybersecurity within their information systems, to take measures to prevent data theft and falsification, and to notify the authorised state body (the State Security Service) upon detecting a cyber attack.⁶

The TIAC, established in 2018 and operating as an institution under public oversight, falls within the class of organisations subject to Article 14. Article 15 of the same Law further requires entities holding data to maintain backup copies for a minimum of three months. Failure to maintain adequate backups that would have permitted reconstruction of a case file following an incident would therefore constitute a breach of a statutory duty, and that breach can serve as evidence of fault for the purpose of the Civil Code Article 333 analysis.⁷

The Presidential Decree No. PP-167 of 31 May 2023 "On Additional Measures to Improve the Cybersecurity System of Critical Information Infrastructure Objects" extended and specified

³ Civil Code of the Republic of Uzbekistan, Arts 14, 324, 333, 337 (contractual liability, losses, fault, force majeure). <https://lex.uz/docs/111181>

⁴ Civil Code of the Republic of Uzbekistan, Arts 985-986, 1000 (tort liability, presumption of fault, strict liability for sources of increased danger). <https://lex.uz/docs/180550>

⁶ Law of the Republic of Uzbekistan "On Cybersecurity" No. ZRU-764 of 15 April 2022 (entered into force 17 July 2022; adopted by the Legislative Chamber 25 February 2022, approved by the Senate 17 March 2022), Arts 3, 14, 15. <https://lex.uz/ru/docs/5960609>

these obligations for Critical Information Infrastructure (CII) subjects. The Decree mandates risk assessment, incident response planning, and regular audits. Arbitral institutions processing significant volumes of confidential commercial data are candidates for CII classification, and once so classified, a failure to comply with the Decree's requirements would materially strengthen a negligence claim under the Civil Code.⁸

The law of electronic documents creates a parallel set of obligations for parties. The Law of the Republic of Uzbekistan "On Electronic Document Management" No. 611-II of 29 April 2004 imposes obligations of storage (Article 16) and protection (Article 17) on participants in electronic document circulation. Where a party transmits an electronically signed document to TIAC's case-management system and that document is later corrupted or deleted by a cyber incident originating from the party's own systems, the party's breach of its storage and protection obligations may shift liability back to it under the comparative-fault framework implied by Article 1004 of the Civil Code, which permits reduction of damages in proportion to the victim's own contributory fault.⁹

Allocative Gaps in the Current Framework. Despite the body of law surveyed above, three significant gaps remain. First, there is no provision in the Law on International Commercial Arbitration No. ZRU-674 of 16 February 2021 (adopted by the Legislative Chamber on 5 August 2020, approved by the Senate on 11 September 2020) that expressly addresses institutional liability for cyber incidents affecting the arbitral process. Article 34 of that Law grants the tribunal broad discretion to determine the admissibility and weight of evidence, but it provides no guidance on what procedural consequences follow when evidence is lost or compromised by an institution's cyber failure.¹⁰

Second, the Law No. ZRU-1003 of 21 November 2024 "On Amendments to Certain Legislative Acts Directed at Improving the System of Working with Digital Evidence" (adopted by the Legislative Chamber on 27 August 2024, approved by the Senate on 24 October 2024), while introducing Articles 89(1)-89(4) on digital evidence into the Civil Procedure Code, operates exclusively in state court proceedings. No equivalent norms govern the handling, presentation, or loss of digital evidence within TIAC proceedings, leaving the tribunal to exercise unguided discretion when cyber incidents corrupt or destroy documentary evidence.¹¹

Third, TIAC's arbitration rules, as publicly available, do not contain a cyber-incident protocol or a force-majeure clause specifically calibrated to digital disruptions. The absence of such a clause means that parties and the institution must rely exclusively on the general provisions of the Civil Code and the cybersecurity legislation, neither of which was designed with the procedural mechanics of arbitration in mind. This creates particular difficulty in cases where a cyber incident delays proceedings: the Civil Code framework addresses financial

⁸ Presidential Decree of the Republic of Uzbekistan "On Additional Measures to Improve the Cybersecurity System of Critical Information Infrastructure Objects" No. PP-167 of 31 May 2023. <https://lex.uz/ru/docs/6479197>

⁹ Law of the Republic of Uzbekistan "On Electronic Document Management" No. 611-II of 29 April 2004, Arts 16-17 (storage and protection of electronic documents); Civil Code, Art. 1004 (contributory fault). <https://lex.uz/docs/165074>

¹⁰ Law of the Republic of Uzbekistan "On International Commercial Arbitration" No. ZRU-674 of 16 February 2021 (adopted by the Legislative Chamber 5 August 2020, approved by the Senate 11 September 2020), Art. 34. <https://lex.uz/docs/5294087>

¹¹ Law of the Republic of Uzbekistan "On Amendments to Certain Legislative Acts Directed at Improving the System of Working with Digital Evidence" No. ZRU-1003 of 21 November 2024 (adopted by the Legislative Chamber 27 August 2024, approved by the Senate 24 October 2024). <https://lex.uz/ru/docs/7228823>

compensation for loss but offers no procedural remedy such as automatic extension of timelines, preservation orders directed at cloud providers, or restitution of a corrupted digital record.

Towards a Statutory Framework: Key Elements. The foregoing analysis suggests that an effective statutory framework for cyber-risk allocation in Uzbek arbitration should address four matters. First, an amendment to the Law on International Commercial Arbitration No. ZRU-674 should introduce an explicit article on institutional cyber-risk obligations, specifying a minimum standard of care (aligned with the requirements of the Law on Cybersecurity No. ZRU-764) and a rule on the allocation of the burden of proof: institutions should bear the burden of demonstrating that a cyber incident was beyond their reasonable control and that they had implemented all required preventive measures.¹²

Second, a corresponding amendment should address the parties' obligations. Parties who submit electronic documents to TIAC proceedings should be required to maintain certified backup copies in accordance with Articles 16 and 17 of the Law on Electronic Document Management No. 611-II, and the tribunal should be empowered to draw adverse inferences where a party's failure to maintain such backups results in evidence being unavailable after a cyber incident attributable to that party's systems.

Third, the amendment should incorporate a cyber force-majeure provision that distinguishes between attacks by sophisticated state-level actors (where the force-majeure defence may be available to the institution) and incidents resulting from failure to implement reasonably available security measures (where the defence should be expressly excluded). This distinction reflects both the general approach of Article 337 of the Civil Code and the standard of care established by Article 14 of the Law on Cybersecurity No. ZRU-764.

Fourth, TIAC should be required to adopt, and publish, a cyber-incident response protocol as a schedule to its arbitration rules. The protocol should specify: a maximum notification period within which the institution must inform parties of a cyber incident affecting their proceedings; procedures for timeline suspension and resumption; and mechanisms for the independent reconstruction or authentication of compromised records. The Law of the Republic of Uzbekistan "On Electronic Digital Signature" No. ZRU-793 of 12 October 2022 (adopted by the Legislative Chamber on 26 July 2022, approved by the Senate on 13 September 2022) provides tools for authentication through certified timestamp services and accredited certification centres that could be deployed in such a protocol.

Conclusion. The allocation of cyber risk in Uzbek arbitration proceedings currently rests on a patchwork of general civil-law principles and sector-specific public-law duties that was not designed for the arbitral context. The Civil Code's fault-based liability framework, the duty-of-care obligations in the Law on Cybersecurity No. ZRU-764 and Presidential Decree No. PP-167, and the storage and protection duties in the Law on Electronic Document Management No. 611-II provide a workable starting point, but they leave critical gaps: no procedural remedies for digital disruption, no explicit institutional liability standard, and no calibrated force-majeure provision.

A targeted amendment to the Law on International Commercial Arbitration No. ZRU-674, supplemented by a mandatory cyber-incident protocol in the TIAC rules, would close these gaps without requiring wholesale reform of the Civil Code. Such an amendment would place Uzbekistan at the forefront of jurisdictions grappling with the intersection of arbitration law and cybersecurity, and would enhance the credibility of TIAC as a venue for high-value international commercial disputes in an era of pervasive digital risk.

Further research is warranted on the comparative experience of arbitral institutions in Singapore, Hong Kong, and Switzerland that have begun developing cyber-incident protocols, on the insurance market's capacity to cover institutional cyber liability in the Uzbek context, and on the interplay between the proposed framework and Uzbekistan's obligations under bilateral investment treaties that include arbitration clauses.

Adabiyotlar, References, Литературы:

1. Born, G. B. (2021). *International Commercial Arbitration* (3rd ed.). Kluwer Law International.
2. Schreuer, C., Malintoppi, L., Reinisch, A., & Sinclair, A. (2009). *The ICSID Convention: A Commentary* (2nd ed.). Cambridge University Press.
3. UNCTAD. (2023). *World Investment Report 2023*. United Nations. <https://unctad.org/wir2023>
4. IBA Guidelines on Party Representation in International Arbitration. (2013). International Bar Association. <https://www.ibanet.org>
5. Republic of Uzbekistan. (1995). Civil Code of the Republic of Uzbekistan, Part One, approved by Law No. 163-I of 21 December 1995 (as amended to date). <https://lex.uz/docs/111181>
6. Republic of Uzbekistan. (1996). Civil Code of the Republic of Uzbekistan, Part Two, approved by Law No. 256-I of 29 August 1996 (as amended to date). <https://lex.uz/docs/180550>
7. Republic of Uzbekistan. (2004). Law "On Electronic Document Management" No. 611-II of 29 April 2004. <https://lex.uz/docs/165074>
8. Republic of Uzbekistan. (2021). Law "On International Commercial Arbitration" No. ZRU-674 of 16 February 2021. <https://lex.uz/docs/5294087>
9. Republic of Uzbekistan. (2022). Law "On Cybersecurity" No. ZRU-764 of 15 April 2022 (entered into force 17 July 2022). <https://lex.uz/ru/docs/5960609>
10. Republic of Uzbekistan. (2022). Law "On Electronic Digital Signature" No. ZRU-793 of 12 October 2022. <https://lex.uz/ru/docs/6234906>
11. Republic of Uzbekistan. (2023). Presidential Decree "On Additional Measures to Improve the Cybersecurity System of Critical Information Infrastructure Objects" No. PP-167 of 31 May 2023. <https://lex.uz/ru/docs/6479197>
12. Republic of Uzbekistan. (2024). Law "On Amendments to Certain Legislative Acts Directed at Improving the System of Working with Digital Evidence" No. ZRU-1003 of 21 November 2024. <https://lex.uz/ru/docs/7228823>
13. Tashkent International Arbitration Centre. (2022). *Annual Report 2022*. <https://tiac.uz/>