“ADOLAT”
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=372

2026-yil
6-son
iyun
ISSN 3093-8546



Soft Law Standards on cybersecurity and their reflection in the Civil Legislation of the Republic of Uzbekistan on International Commercial Arbitration

Begaim Kaibyldaeva,
Tashkent State University of Law
Independent Researcher
e-mail: begaimkaibyldaeva@gmail.com

Аннотация. Axborot texnologiyalarining jadal rivojlanishi va raqamli kommunikatsiyalarning globallashuvi kiberxavfsizlikni xalqaro tijorat arbitrajining eng dolzarb muammolaridan biriga aylantirdi. Ushbu maqolada UNCITRAL, Xalqaro savdo palatasi va Cybersecurity Tech Accord kabi tashkilotlar tomonidan ishlab chiqilgan ko‘rsatmalar, namunaviy qonunlar, tavsiyalar va eng yaxshi amaliyotlar to‘plamini o‘z ichiga olgan “yumshoq huquq” vositalarining arbitraj ishlarida kiberxavfsizlikni tartibga solishga ta’siri o‘rganiladi. Ma’lumotlarni himoya qilish, elektron kommunikatsiyalar xavfsizligi va arbitraj ishlarining maxfiyligi sohasidagi “yumshoq huquq” standartlarining O‘zbekiston Respublikasining “Xalqaro tijorat arbitraji to‘g‘risida”gi qonunida qay darajada aks etganligi tahlil qilinadi.

Калит сўзлар. yumshoq huquq, kiberxavfsizlik, xalqaro tijorat arbitraji, UNCITRAL, ma’lumotlarni himoya qilish, maxfiylik, raqamli arbitraj, O‘zbekiston, fuqarolik qonunchiligi, axborot xavfsizligi.

Аннотация. Стремительное развитие информационных технологий и глобализация цифровых коммуникаций превратили кибербезопасность в одну из наиболее актуальных проблем международного коммерческого арбитража. В настоящей статье исследуется влияние инструментов «мягкого права», включая руководящие принципы, типовые законы, рекомендации и документы лучших практик, разработанных такими организациями, как ЮНСИТРАЛ, Международная торговая палата и Cybersecurity Tech Accord, на регулирование вопросов кибербезопасности в арбитражном производстве. Анализируется степень отражения стандартов «мягкого права» в области защиты данных, безопасности электронных коммуникаций и конфиденциальности арбитражного разбирательства в гражданском законодательстве Республики Узбекистан о международном коммерческом арбитраже. Выявлены существующие законодательные пробелы и предложены конкретные меры по реформированию с целью приведения арбитражного законодательства Узбекистана в соответствие с современными требованиями кибербезопасности.

Ключевые слова. мягкое право, кибербезопасность, международный коммерческий арбитраж, ЮНСИТРАЛ, защита данных, конфиденциальность, цифровой арбитраж, Узбекистан, гражданское законодательство, информационная безопасность.

Annotation. The rapid development of information technologies and the globalisation of digital communications have made cybersecurity one of the most pressing concerns in international commercial arbitration. This article examines the influence of soft law instruments, including guidelines, model laws, recommendations, and best practice frameworks developed by organisations such as UNCITRAL, the International Chamber of Commerce, and the Cybersecurity Tech Accord, on the regulation of cybersecurity in arbitral proceedings. The article analyses the extent to which soft law standards on data protection, secure electronic communications, and confidentiality of arbitral proceedings are reflected in the civil legislation of the Republic of Uzbekistan governing international commercial arbitration. It identifies existing legislative gaps and proposes targeted reforms to ensure that Uzbekistan's arbitration framework meets contemporary cybersecurity requirements.

Keywords. soft law, cybersecurity, international commercial arbitration, UNCITRAL, data protection, confidentiality, digital arbitration, Uzbekistan, civil legislation, information security.

Introduction. The digitalisation of international trade and dispute resolution has fundamentally transformed the environment in which international commercial arbitration operates. Arbitral proceedings today routinely involve the transmission of sensitive commercial secrets, personal data, witness statements, and legal submissions across international borders via electronic means. The confidentiality and integrity of these communications, long regarded as a foundational principle of arbitration, are now exposed to a range of cybersecurity threats that traditional legal frameworks were not designed to address.

In response to this challenge, international organisations and arbitral institutions have developed a body of soft law instruments setting standards for cybersecurity in arbitration. Soft law, as distinguished from binding treaty obligations and national legislation, comprises guidelines, recommendations, protocols, and best practice documents that carry significant normative authority without formal legal force. The soft law landscape on cybersecurity in arbitration includes, among others, the UNCITRAL Notes on Organizing Arbitral Proceedings (2016 edition), the International Chamber of Commerce Cybersecurity Guidelines for Virtual Hearings (2020), the ICC Guidance Note on Possible Measures Aimed at Mitigating the Effects of the COVID-19 Pandemic (2020), and the Prague Rules on the Efficient Conduct of Proceedings in International Arbitration.

The Republic of Uzbekistan has undertaken significant reforms of its arbitration legislation in recent years. The Law of the Republic of Uzbekistan on International Commercial Arbitration (hereinafter the ICA Law), adopted in 2021 and amended on several occasions, provides the primary statutory

framework for international arbitration seated in Uzbekistan. Presidential Decree No. UP-60 of January 28, 2022, on additional measures for the development of the investment environment, and the broader digital transformation programme launched under the Digital Uzbekistan 2030 strategy, signal a governmental commitment to modernising the legal environment for commercial dispute resolution. [1] However, the extent to which Uzbekistan's civil legislation on international commercial arbitration reflects contemporary soft law standards on cybersecurity remains a largely unexplored question in legal scholarship.

This article pursues three objectives. First, it maps the principal soft law standards on cybersecurity relevant to international commercial arbitration. Second, it analyses the degree to which these standards are reflected in, or consistent with, Uzbekistan's current civil legislation. Third, it identifies legislative gaps and proposes targeted reforms. The article draws on comparative analysis of leading national arbitration laws, including the UNCITRAL Model Law on International Commercial Arbitration (1985, as amended in 2006), English arbitration law, and the Singaporean framework, which offers the most advanced integrated approach to cybersecurity in arbitration.

Soft Law and Cybersecurity in International Commercial Arbitration: Conceptual Foundations. The concept of soft law occupies a contested but important position in international legal theory. Snyder defined soft law as rules of conduct which, in principle, have no legally binding force but which nevertheless may have practical effects. [2] In the context of international arbitration, soft law instruments perform several distinctive functions: they harmonise practice across jurisdictions that would otherwise resist binding treaty obligations; they respond more rapidly to technological developments than domestic legislation; and they shape the legitimate expectations of parties and arbitral tribunals, gradually acquiring normative authority through repeated practice.

Cybersecurity threats to arbitral proceedings take several distinct forms. The first is the unauthorised interception of arbitration communications, including hacking of email correspondence, witness statements, and pleadings during transmission. The second is the compromise of virtual hearing platforms, including eavesdropping, recording, or disruption of online proceedings. The third is the ransomware attack or data breach directed at arbitral institutions or parties' legal counsel, resulting in the exposure or destruction of arbitration-related data. The fourth is the manipulation of electronic evidence through forgery or alteration of digitally submitted documents. Each of these threats carries distinct legal implications for the integrity and confidentiality of arbitral proceedings.

The normative response to these threats at the international level has been largely accomplished through soft law. The UNCITRAL Notes on Organizing Arbitral Proceedings, while not addressing cybersecurity specifically in their 1996 version, were updated in 2016 to include guidance on electronic communications and data management. The ICC Cybersecurity Guidelines for Virtual Hearings, published in 2020 in direct response to the COVID-19 pandemic's acceleration of online arbitration, establish detailed recommendations on platform security, participant verification, and the

technical standards for secure virtual hearings. [3] The ICC Commission on Arbitration and ADR Task Force on Data Delivery and Cybersecurity has further developed guidance on cybersecurity protocols and incident response procedures. The Cybersecurity Tech Accord, while primarily directed at the technology industry, articulates principles of user protection and security-by-design that have influenced the thinking of arbitral institutions about their own infrastructure obligations.

The Current State of Uzbekistan's Civil Legislation on International Commercial Arbitration and Cybersecurity. Uzbekistan's primary legislative instrument governing international commercial arbitration is the "Law on International Commercial Arbitration" No. LRU-674 of February 16, 2021, which is closely modelled on the UNCITRAL Model Law. [4] The Law addresses the foundational principles of party autonomy, kompetenz-kompetenz, the separability of the arbitration clause, procedural flexibility, and the limited grounds for judicial intervention. It also provides rules on the recognition and enforcement of foreign arbitral awards consistent with the 1958 New York Convention, to which Uzbekistan acceded in 1995.

A careful examination of the ICA Law reveals that it contains no specific provisions addressing cybersecurity. The Law's provisions on the conduct of proceedings, including the delivery of written communications under Article 3, the conduct of hearings under Article 24, and the rules on evidence, are drafted without reference to electronic communications, digital security, or data protection. This reflects the historical context of the Law's adoption in 2021, when virtual hearings and electronic arbitration were not yet standard practice. However, the absence of any cybersecurity-related amendment since that date represents a significant legislative gap in light of developments in arbitration practice.

The broader civil legislation of Uzbekistan includes several instruments with potential relevance to cybersecurity in arbitration. Law on Electronic Digital Signature No. LRU-793, October 12, 2022, as amended) establishes the legal validity of electronic documents and digital signatures. [5] "The Law on Cybersecurity No. LRU-764, April 15, 2022." provides a general framework for information security obligations.[6] However, none of these instruments specifically addresses the cybersecurity obligations of arbitral institutions, arbitrators, or parties to arbitration proceedings seated in Uzbekistan.

The Civil Procedure Code of the Republic of Uzbekistan and the Code of Economic Procedure, which govern judicial proceedings in Uzbekistan, have been amended in recent years to accommodate electronic filing and digital document management. [7] These reforms provide useful analogical precedent for cybersecurity regulation in arbitration, but their provisions are not directly applicable to private arbitral proceedings and do not constitute soft law reflection in the arbitration framework.

Analysis of Key Soft Law Standards and Their Reflection in Uzbek Arbitration Law. The UNCITRAL Model Law on Electronic Commerce (1996) and the UNCITRAL Model Law on Electronic Signatures (2001) established the foundational principles of functional equivalence and technology neutrality that underpin the legal treatment of electronic communications in international trade and arbitration. [8] The Model Law on Electronic Commerce's principle that electronic communications shall not be denied

legal effect solely on the grounds that they are in electronic form has been adopted in Uzbekistan's Law on Electronic Document Circulation and Electronic Digital Signature, providing a basis for the recognition of electronically transmitted arbitration documents.

However, the UNCITRAL Model Law's approach to confidentiality in arbitration, articulated in Article 2A’s general principle of good faith and in the travaux preparatoires to the 2006 amendments, has not been explicitly incorporated into the Uzbek ICA Law. The Uzbek Law does not contain a general confidentiality obligation binding on parties, arbitrators, and institutions. This represents a significant divergence from contemporary soft law standards. The ICC Rules of Arbitration (2021), the Singapore International Arbitration Centre Rules (SIAC, 2016), and the London Court of International Arbitration Rules (LCIA, 2020) all impose explicit confidentiality obligations that encompass electronically stored and transmitted arbitration materials. [9]

The ICC Cybersecurity Guidelines for Virtual Hearings recommend that arbitral tribunals adopt a cybersecurity protocol at the outset of proceedings, specifying the platform to be used for virtual hearings, the authentication procedures for participants, the prohibition on unauthorised recording, and the procedures to be followed in the event of a security incident. [3] These recommendations reflect a soft law consensus on minimum cybersecurity standards for virtual arbitration proceedings. The Uzbek ICA Law contains no equivalent provision empowering tribunals to adopt such protocols or imposing any baseline cybersecurity obligation. The Law's general provision in Article 19 granting parties autonomy to agree on the procedure, and the tribunal's residual power to conduct proceedings in such a manner as it considers appropriate, provides an indirect basis for the adoption of cybersecurity protocols by agreement, but does not constitute a statutory reflection of the relevant soft law standard.

The UNCITRAL Technical Notes on Online Dispute Resolution (2017) address the specific challenges of electronic proceedings, including data security, system reliability, and the verification of parties' identities in online processes. [10] While directed primarily at consumer online dispute resolution, the Technical Notes have influenced the development of cybersecurity standards for international commercial arbitration. Uzbekistan has not adopted implementing legislation for the UNCITRAL Technical Notes, and the ICA Law does not address the specific challenges identified therein.

Data protection constitutes a distinct dimension of cybersecurity soft law with direct relevance to arbitration. The General Data Protection Regulation of the European Union (GDPR, 2016/679), while not directly applicable in Uzbekistan, has profoundly shaped global standards on the processing of personal data, including data processed in the context of international commercial disputes. [11] The ICC and SIAC have both updated their rules and guidance to address GDPR compliance in arbitration proceedings involving EU-based parties or data. Uzbekistan’s Personal Data Law (Law No. LRU-547 of July 2, 2019) establishes a national framework for personal data protection. [12] However, the Law does not address the specific context of data processed in international arbitration proceedings, and the ICA Law contains no cross-reference to data protection obligations. This gap is particularly significant because arbitration proceedings frequently involve the processing

of personal data belonging to natural persons in the context of corporate disputes.

Comparative Analysis: Leading Jurisdictions and Their Approaches. Singapore has emerged as the leading jurisdiction for the integration of cybersecurity standards into arbitration law and institutional practice. The Singapore International Arbitration Centre has adopted detailed cybersecurity protocols as part of its practice notes, requiring parties to agree on cybersecurity measures and empowering the tribunal to make procedural orders on information security. [13] The Singaporean Model AI Governance Framework, while focused on artificial intelligence, reflects a broader regulatory philosophy of integrating technology governance standards into commercial dispute resolution frameworks. Hong Kong's Law Reform Commission has similarly recommended amendments to the Hong Kong Arbitration Ordinance to address electronic proceedings and cybersecurity. [14]

England and Wales present a contrasting model. The Arbitration Act 1996, currently under review by the Law Commission, does not specifically address cybersecurity, but the LCIA has developed detailed cybersecurity provisions through its institutional rules and practice guidance. The Law Commission's 2023 review of the Arbitration Act considered, but ultimately did not recommend, the introduction of statutory cybersecurity obligations, preferring to leave the matter to institutional rules and party autonomy. [15] This approach reflects a legitimate regulatory choice, but it presupposes a highly developed ecosystem of institutional rules and practitioner awareness that Uzbekistan has not yet fully developed.

Kazakhstan, as a neighbouring jurisdiction with a shared legal heritage and a comparable stage of digital development, presents a particularly relevant comparator. The Kazakhstan International Arbitration Centre (KIAC) has adopted procedural rules that incorporate provisions on electronic communications and document management, though comprehensive cybersecurity protocols comparable to those of the ICC or SIAC have not yet been formally integrated. [16] The Kazakhstani experience suggests that jurisdictions in the Central Asian region are beginning to engage with cybersecurity in arbitration, but that legislative reform has generally lagged behind institutional practice.

Identified Legislative Gaps and Proposals for Reform. The foregoing analysis identifies five principal legislative gaps in Uzbekistan's civil legislation on international commercial arbitration from the perspective of soft law standards on cybersecurity.

First, the ICA Law contains no confidentiality obligation encompassing electronically stored and transmitted arbitration materials. The introduction of a general statutory confidentiality obligation, as recommended by UNCITRAL and adopted in many leading arbitration laws, is the most fundamental reform required. Such an obligation should cover all parties, arbitrators, arbitral institutions, and any other persons involved in the proceedings, and should explicitly extend to all electronic communications, hearing recordings, and documentary evidence submitted in digital form.

Second, the ICA Law should be amended to authorise arbitral tribunals to adopt cybersecurity protocols as part of their procedural orders. This amendment would give statutory grounding to the ICC Guidelines'

recommendation and would provide a clear legal basis for tribunals to impose binding cybersecurity requirements on the parties. The amendment could be modelled on Article 17 of the UNCITRAL Model Law concerning interim measures, adapted to address procedural information security requirements.

Third, Uzbekistan should develop a cross-reference mechanism linking the ICA Law to the relevant provisions of the Law on Information and the Guarantee of Information Security and the Personal Data Law. At present, the relationship between these bodies of legislation and the ICA Law is legally uncertain. A specific provision clarifying that internationally recognised standards on information security are applicable to arbitration proceedings seated in Uzbekistan would address this gap and align Uzbek law with the approach of more developed arbitration frameworks.

Fourth, the Law on Electronic Document Circulation and Electronic Digital Signature should be amended or supplemented by implementing regulations to address the specific requirements of electronic evidence in arbitration proceedings, including chain of custody requirements, metadata preservation, and the admissibility of electronically authenticated documents. The UNCITRAL Model Law on Electronic Transferable Records (2017) provides relevant guidance in this regard. [17]

Fifth, Uzbekistan should engage actively with UNCITRAL's ongoing work on dispute resolution in the digital economy, including the work of Working Group II on Dispute Settlement and Working Group III on Investor-State Dispute Settlement Reform, both of which are addressing cybersecurity and data protection issues. Active participation in these processes would enable Uzbekistan to shape emerging soft law standards in a manner consistent with its national interests and to receive early guidance on legislative best practice.

Conclusion. Soft law instruments developed by UNCITRAL, the ICC, the SIAC, and other international bodies have established a clear normative framework for cybersecurity in international commercial arbitration. This framework encompasses confidentiality obligations, tribunal powers to adopt cybersecurity protocols, data protection requirements, and standards for the security of virtual hearings and electronic evidence. Uzbekistan's current civil legislation on international commercial arbitration does not adequately reflect these standards. The ICA Law, adopted in 2021 and not substantively amended in relation to electronic proceedings or cybersecurity, contains no confidentiality obligation, no tribunal power to adopt cybersecurity protocols, and no cross-reference to the country's broader information security and data protection legislation.

The comparative analysis of Singapore, England, Kazakhstan, and other jurisdictions confirms that legislative reform in this area is both necessary and achievable. The reforms proposed in this article, namely the introduction of a statutory confidentiality obligation, the authorisation of tribunal cybersecurity protocols, a legislative cross-reference mechanism, enhanced electronic evidence rules, and active engagement with UNCITRAL's digital economy work programme, constitute a coherent and proportionate legislative programme. Implementation of these reforms would enhance the attractiveness of Uzbekistan as a seat of international commercial arbitration, protect the legitimate interests of parties and arbitrators, and position Uzbekistan as a constructive participant in the development of international soft law standards

on cybersecurity in dispute resolution.

REFERENCES:

1. Republic of Uzbekistan. Decree of the President of the Republic of Uzbekistan “On the Development Strategy of New Uzbekistan for 2022–2026.” No. PF-60, January 28, 2022.

2. Snyder, F. (1993). The effectiveness of European Community law: Institutions, processes, tools and techniques. Modern Law Review, 56(1), 19-54.

3. International Chamber of Commerce. (2020). ICC Cybersecurity Guidelines for Virtual Hearings. ICC Commission on Arbitration and ADR.

4. Republic of Uzbekistan. Law on International Commercial Arbitration No. LRU-674, February 16, 2021.

5. Republic of Uzbekistan. Law on Electronic Digital Signature No. LRU-793, October 12, 2022.

6. Republic of Uzbekistan. Law on Cybersecurity No. LRU-764, April 15, 2022.

7. Republic of Uzbekistan. Economic Procedure Code, approved by Law No. LRU-461, January 24, 2018 (as amended).

8. UNCITRAL. (1996). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment. United Nations. (UNCITRAL Model Law on Electronic Signatures, 2001, adopted by the same body.)

9. International Chamber of Commerce. (2021). ICC Rules of Arbitration. ICC Publication No. 874. (Singapore International Arbitration Centre Rules, 6th ed., 2016; LCIA Arbitration Rules, 2020, adopted by respective institutions.)

10. UNCITRAL. (2017). UNCITRAL Technical Notes on Online Dispute Resolution. United Nations.

11. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119/1.

12. Republic of Uzbekistan. Law on Personal Data No. LRU-547 of July 2, 2019. https://lex.uz

13. Singapore International Arbitration Centre. (2021). SIAC Practice Note on the Conduct of Virtual Hearings. SIAC.

14. Hong Kong Law Reform Commission. (2021). Report on Online Dispute Resolution. HKLRC.

15. Law Commission of England and Wales. (2023). Review of the Arbitration Act 1996: Report (Law Com No. 413). The Stationery Office.

16. Kazakhstan International Arbitration Centre. (2022). KIAC Rules of Arbitration. KIAC.

17. UNCITRAL. (2017). UNCITRAL Model Law on Electronic Transferable Records. United Nations.