4 INTERNATIONAL AND COMPARATIVE LAW
ХАЛЫҚАРАЛЫҚ ЖӘНЕ САЛЫСТЫРМАЛЫ ҚҰҚЫҚ
МЕЖДУНАРОДНОЕ И СРАВНИТЕЛЬНОЕ ПРАВО

IRSTI 10.15.03
UDC 341.763
JEL K39

https://doi.org/10.46914/2959-4197-2025-1-1-48-53

LOU Y.,*[1]
master's student.
*e-mail: louy@aliyun.com
ORCID ID: 0009-0006-8382-5607
YERGALI A.M.,[1]
PhD, associate professor.
e-mail: yergali.adlet@gmail.com
ORCID ID: 0000-0001-8530-3905
[1]Al-Farabi Kazakh National University,
Almaty, Kazakhstan

THE DEVELOPMENT OF A LEGAL FRAMEWORK FOR DATA SECURITY COOPERATION WITHIN THE SHANGHAI COOPERATION ORGANIZATION

Abstract

With the Shanghai Cooperation Organization's (SCO) progressive enlargement, its geographic scope extends from Central Asia to South Asia and adjacent regions. This broadening highlights the necessity of developing a standardized data governance architecture as the cornerstone for digital economic advancement within the SCO framework. The current landscape, characterized by heterogeneous regulatory approaches among member nations and insufficient multilateral coordination mechanisms, necessitates urgent institutional innovation. Three foundational pillars emerge for establishing this cooperative regime: Formulating cross-border data governance protocols; Creating multi-tiered legislative coordination structures; Implementing comprehensive collaborative security standards. Given China's prominent role in digital transformation, it should proactively advance its strategic blueprint through multilateral platforms, proposing innovative solutions in SCO negotiations while fostering collective security paradigms that benefit all stakeholders.

Key words: SCO, data security cooperation, data hegemony, digital economy, International Organizations.

Introduction

Between its establishment in 2001 and 2020, the Shanghai Cooperation Organization (SCO) member states witnessed a more than tenfold increase in collective GDP and a near ninefold rise in merchandise trade volumes, demonstrating the bloc's growing geopolitical and economic clout on the world stage [1]. Over the past twenty years, the Shanghai Cooperation Organization (SCO) member states have implemented multidimensional collaboration spanning security, economic integration, political coordination, social development, and cultural exchange. This cooperation has demonstrated progressive expansion in operational breadth, standardization of procedures, institutionalized openness, and mechanism optimization. Evolving from its original informal consultative format, the SCO has systematically developed summit mechanisms, refined organizational architecture, and codified cooperative legal frameworks. As stipulated in the SCO Charter, its institutional configuration

incorporates multiple permanent bodies and specialized agencies. Functioning as a multilateral regional entity, the legal cooperation framework constitutes an essential operational foundation for the organization's sustainable development.

The SCO's cooperative paradigm has undergone significant evolution in both substantive domains and implementation modalities. Notably, the digital economy has emerged as a critical frontier, where data security challenges – including unauthorized access vulnerabilities and transnational data transmission risks – have become prioritized agenda items. This necessitates the formulation of adaptive regulatory frameworks to govern data security within big data ecosystems. Given the deep integration of digital technologies across economic, social, and governance systems, the SCO currently faces critical institutional gaps in coordinating data security governance across member states [2].

Current assessments reveal that only select member states – notably China, Russia, and India – possess requisite technical infrastructure and legislative frameworks for comprehensive data security management. The majority demonstrate insufficient legal capacities to address contemporary data security challenges, creating pressing demands for regulatory harmonization. An effective SCO data security cooperation architecture should integrate four core components: organizational coordination platforms, sector-specific regulatory agreements, mutual recognition protocols for security measures, and transnational dispute resolution mechanisms. Compared with domestic data governance systems, SCO-level cooperation inherently involves greater complexity, requiring dynamic equilibrium between regulatory harmonization and national sovereignty considerations.

Materials and methods

The envisioned legal framework for SCO data security cooperation must fulfill dual functions: first, supporting member states in developing context-specific national data protection systems pursuing the dual objectives of "robust data safeguarding" and "value-driven data utilization"; second, establishing interoperable mechanisms for cross-border sharing and mutual benefit realization of data resources. The relativity theory of security posits that data security constitutes the necessary foundation for advancing members' digital economies rather than representing the terminal objective of international collaboration [2]. Consequently, the SCO should eschew absolutist conceptions of data security, instead cultivating legal mechanisms that balance security imperatives with data accessibility requirements.

This legal architecture must demonstrate dynamic adaptability to ensure sustainable evolution. Conventional challenges such as data breaches and integrity violations – manifesting as static security risks – can be addressed through established legal instruments. However, the SCO framework requires proactive regulatory architecture capable of anticipating emerging technological paradigms, thereby maintaining relevance in the face of rapid digital transformation. Such forward-looking design principles will ensure the mechanism's continued effectiveness as both a governance tool and an enabler of regional digital integration.

Results and discussion

The digital economy has emerged as a pivotal arena in global developmental competition. SCO member states have strategically integrated digital economic growth into their national agendas, recognizing that a robust legal framework for data security cooperation serves as both a foundational safeguard for intra-bloc digital integration and a critical enabler of external competitiveness. The institutionalization of such mechanisms has become indispensable to SCO digital collaboration, with multilateral participation in their construction being vital for ensuring internal data governance efficacy and enhancing collective bargaining power in the global digital economy.

1 Jurisdictional Heterogeneity in Data Security Regulations

SCO member states universally acknowledge the strategic significance of data resources, having elevated data security governance to matters of "national security" and "competitive advantage". Nevertheless, substantive divergences persist in their regulatory architectures.

1.1 Asymmetric Digital Infrastructure Development

First, digital infrastructure distribution within the SCO exhibits pronounced imbalance. Mobile connectivity dominates user engagement, while platform ecosystems remain predominantly controlled

by U.S. entities. Regional internet penetration stands at 40%, with 76% of users accessing services via mobile devices. Over 60% frequent international social platforms (e.g., Facebook, Twitter, WhatsApp) alongside domestic alternatives. Huawei's 2019 Digital Economy Index categorizes China, Russia, and Kazakhstan as digital acceleration economies, contrasting with India and Pakistan's status as emerging digital markets [3].

Second, digital economic maturity demonstrates marked stratification:

Tier 1 (Medium-High): China

Tier 2 (Medium): India, Russia, Kazakhstan, Pakistan

Tier 3 (Medium-Low): Uzbekistan, Kyrgyzstan, Tajikistan

Notably, Uzbekistan has prioritized bandwidth enhancement and infrastructure investment, whereas Tajikistan confronts acute connectivity challenges—70% of its mountainous population lacks broadband access, with only 35% utilizing mobile internet [3].

Third, regulatory sophistication remains uneven. Excluding China, India, and Russia, most SCO members exhibit underdeveloped digital governance frameworks, particularly regarding data security legislation.

1.2 Divergent National Regulatory Paradigms

Member states have formulated distinct data security strategies reflecting domestic priorities:

China: Champions comprehensive modernization, emphasizing digital sovereignty, citizen data rights, and global governance reform.

India: Focuses on technological innovation and supervisory mechanisms for public-private sectors.

Russia: Legislates holistic protections spanning national security, economic data, and military intelligence.

Kazakhstan: Develops threat-responsive legal frameworks with emergency protocols.

Pakistan: Combats cyber intrusions through standardized governance frameworks.

Kyrgyzstan (2019–2023): Phased implementation of anti-espionage measures and societal risk mitigation.

Tajikistan: Prioritizes transparent personal data governance across lifecycle stages.

Uzbekistan: Implements institutional capacity-building and cybersecurity education integration.

2 Institutional Deficiencies in SCO Data Security Cooperation

Despite consensus on data security's strategic importance, the SCO lacks cohesive regulatory architecture, resulting in fragmented governance, conflicting national agendas, and inadequate implementation frameworks. This institutional void complicates multilateral coordination, underscoring the urgency of mechanism development.

2.1 Global Regulatory Fragmentation

The absence of SCO coordination mirrors broader international discord. Developed economies exhibit stark policy contrasts – exemplified by U.S.-EU disputes over data flow governance. While agreements like the Digital Economy Partnership Agreement (DEPA) provide detailed provisions, multilateral frameworks (e.g., WTO services trade rules) remain underdeveloped [7].

Data localization measures, which have proliferated globally (post-2017 increase exceeding 100%), often hinder cross-border flows without enhancing protection. SCO members face compounded challenges from conflicting bilateral agreements and eroding global consensus, stifling both regulatory harmonization and digital economic growth [4].

2.2 Hegemonic Data Governance Practices

Digital power asymmetries, particularly U.S. data dominance, manifest through three mechanisms:

Surveillance Overreach: Extraterritorial jurisdiction justified under national security pretexts [5].

Politicized Standards: Ideological framing of data security norms [6].

Economic Coercion: Strategic control over global data flows to maintain traditional power structures.

These practices undermine multilateral cooperation and necessitate SCO countermeasures through institutionalized collaboration.

2.3 Structural Weaknesses in SCO Governance

Current cooperation remains largely declaratory, characterized by:

Absence of Binding Instruments: No dedicated legal framework for enforcement.

Platform Deficiencies: Initiatives lack operational implementation mechanisms.

Shallow Cooperation Depth: Lagging behind mature systems (e.g., U.S.-EU frameworks).

Geopolitical Complexity: U.S.-led data hegemony complicates threat responses.

The convergence of these challenges underscores the imperative for the SCO to develop adaptive legal frameworks that reconcile sovereignty concerns with collective security requirements, ensuring sustainable digital economic advancement.

Conclusion

Data security cooperation constitutes the institutional cornerstone for advancing the digital economy within the Shanghai Cooperation Organization (SCO). Establishing a multilateral legal mechanism for data security governance represents an urgent priority for the bloc's sustainable development.

1 Foundational Principles of the SCO Data Security Legal Architecture

Principle of Data Sovereignty: As the bedrock principle, data sovereignty recognizes data security as a strategic asset intrinsically linked to national security and societal stability. This encompasses dual dimensions: domestic regulatory autonomy and international collaborative governance [3].

Principle of Secure Development Synergy: Digital economic advancement must synchronize with robust data protection frameworks, safeguarding national, corporate, and individual data integrity to ensure sustainable growth.

Principle of Equitable Collaboration: Member states shall pursue reciprocal benefits through egalitarian cooperation, prioritizing collective progress over unilateral advantages.

Principle of Consultative Governance: Building upon the 2009 Agreement on International Information Security Cooperation, this principle emphasizes institutionalized dialogue to construct adaptable legal frameworks aligned with multilateral needs [7].

2 Structural Framework for SCO Data Security Governance

Mutually Beneficial Governance Paradigm: Rejecting unilateralism and hegemonic practices, this paradigm advocates data sovereignty preservation and equitable legal system development.

Institutionalized Cooperation Platforms: Establish specialized committees (e.g., Data Security Oversight Commission with subcommittees for Trade, Intellectual Property, and Investment) to facilitate regulatory harmonization, cross-border enforcement, and capacity-building initiatives [3, 7].

Digital Supply Chain Security Regime: Implement standardized protocols for digital product/service supply chains to mitigate operational risks and ensure ecosystem stability.

Personal Data Protection Mechanisms: Leverage technological safeguards and legislative measures to prevent unauthorized data access/modification, thereby protecting citizen privacy rights across member states.

3 Implementation Pathways for Legal System Development

Legal Interoperability Enhancement: Align SCO frameworks with national legislations such as China's Cybersecurity Law and Russia-Kazakhstan digital economy strategies to ensure regulatory coherence [8].

Institutionalized Collaborative Governance: Formalize cooperation through a Data Security Charter articulating operational principles and decision-making protocols [9].

Dispute Resolution Adjudicative Framework: Establish specialized arbitration bodies employing consultative mediation and binding arbitration to resolve cross-jurisdictional data conflicts [9].

4 China's Strategic Leadership Initiatives

Multilateral Rule-Based Engagement: Advocate UN/WTO-aligned reforms in global data governance, prioritizing bilateral/regional agreement networks that respect data sovereignty.

Negotiation Platform Optimization: Leverage instruments like the Global Data Security Initiative to strengthen SCO legal coordination mechanisms [10].

Shared Security Community Building: Promote a cooperative paradigm balancing data rights equality, sovereignty protection, and developmental synergy, offering China's institutional innovation model for SCO digital integration [11].

In the era of digital transformation, data security governance has emerged as a pivotal domain of international strategic competition. As both a leading digital economy and SCO stakeholder, China bears responsibility for spearheading standardized cooperation frameworks, contributing its normative governance wisdom to shape the SCO's data security architectural design. Through proactive mechanism innovation and multilateral consensus-building, China can catalyze the evolution of equitable, future-oriented data governance regimes within the Eurasian digital landscape.

REFERENCES

1 Huaqin L. Enhancing the New Space for Regional Economic Cooperation of the Shanghai Cooperation Organization through the Digital Economy // Academic Journal of Russian Studies. 2022, no. 3. URL: https://d.wanfangdata.com.cn/periodical/elsxk202203001

2 Yuejin L. The Concept and Ideology of a Comprehensive Security Framework under Systems Thinking // People's Tribune. 2021, no. 8. URL: https://www.cnki.net/kcms/detail/detail.aspx?filename=RMLT202108004&dbcode=CJFQ&dbname=CJFD2021&v=

3 Developing the Digital Economy of the Shanghai Cooperation Organization: A Perspective Based on Data Security Cooperation. URL: https://www.chinaaet.com/article/3000137861

4 How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. ITIF. URL: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

5 Kwet M. Digital Colonialism: US Empire and the New Imperialism in the Global South // Race & Class. 2021, no. 3. URL: https://journals.sagepub.com/doi/10.1177/0306396818823172

6 Haoyan L. Data Hegemony and the New Form of Digital Imperialism // Contemporary Economic Research. 2021, no. 2. URL: https://d.wanfangdata.com.cn/periodical/ddjjyj202102007

7 Statement of the Council of Heads of State of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security. 2020. URL: https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/dozys_673577/dqzzoys_673581/shhz_673583/zywj_673595/202011/t20201110_7627465.shtml

8 Haiyan W. The Mechanism Construction and Challenges of Information Security Cooperation within the Shanghai Cooperation Organization // China Information Security. 2021, no. 8. URL: https://wenku.baidu.com/view/6f48ba9c1a2e453610661ed9ad51f01dc381577c.html

9 Shumei Y. Research on the Law System of International Civil Nuclear Energy Security // Wuhan University International Law Review. 2017, no. 4. URL: https://xueshu.baidu.com/usercenter/paper/show?paperid=868618d84797da01cfedaf5c3162a455&site=xueshu_se

10 "China + Five Central Asian Countries" Data Security Cooperation Initiative – Ministry of Foreign Affairs of the People's Republic of China. 2022. URL: https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/202206/t20220609_10700811.shtml.

11 Xinyi L. The Study of the Construction of Global Digital Economy Rule System from the Perspective of International Law // Journal of Chengdu Institute of Public Administration. 2020, no. 6. URL: https://d.wanfangdata.com.cn/periodical/cdxzxyxb202006010

ЛОУ Ю.,*[1]
магистрант.
*e-mail: louy@aliyun.com
Orcid id: 0009-0006-8382-5607
ЕРГАЛИ А.М.,[1]
PhD, доцент.
e-mail: yergali.adlet@gmail.com
Orcid id: 0000-0001-8530-3905
[1]Казахский национальный
университет им. аль-Фараби,
г. Алматы, Казахстан

ПОСТРОЕНИЕ ПРАВОВОГО МЕХАНИЗМА СОТРУДНИЧЕСТВА В ОБЛАСТИ БЕЗОПАСНОСТИ ДАННЫХ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА

Аннотация

В связи с постепенным расширением Шанхайской организации сотрудничества (ШОС) ее географический охват распространился от Центральной Азии до Южной Азии и прилегающих регионов. Это расширение подчёркивает необходимость разработки стандартизированной архитектуры управления данными, являющейся краеугольным камнем цифрового экономического развития в рамках ШОС. Нынешняя ситуация, характеризующаяся гетерогенными регуляторными подходами среди государств-членов и недостаточностью многосторонних координационных механизмов, требует срочных институциональных инноваций. Выделя-

ются три основные опоры для создания данного кооперативного режима: разработка трансграничных протоколов управления данными; создание многоуровневых структур законодательной координации; внедрение комплексных стандартов совместной безопасности. Учитывая видную роль Китая в цифровой трансформации, он должен активно продвигать свою стратегическую концепцию через многосторонние платформы, предлагая инновационные решения в рамках переговоров ШОС и способствуя формированию коллективных парадигм безопасности, приносящих выгоду всем заинтересованным сторонам.

Ключевые слова: ШОС, сотрудничество в области безопасности данных, гегемония данных, цифровая экономика, международные организации.

ЛОУ Ю.,*[1]
магистрант.
*e-mail: louy@aliyun.com
ORCID ID: 0009-0006-8382-5607
ЕРҒАЛИ Ә.М.,1
PhD, доцент
e-mail: yergali.adlet@gmail.com
ORCID ID: 0000-0001-8530-3905
[1]әл-Фараби атындағы
Қазақ ұлттық университеті,
Алматы қ., Қазақстан

ШАНХАЙ ЫНТЫМАҚТАСТЫҚ ҰЙЫМЫ ДЕРЕКТЕР ҚАУІПСІЗДІГІ БОЙЫНША ЫНТЫМАҚТАСТЫҚТЫҢ ҚҰҚЫҚТЫҚ МЕХАНИЗМІН ҚҰРУ

Аннотация

Шанхай ынтымақтастық ұйымының (ШЫҰ) біртіндеп кеңеюімен оның географиялық ауқымы Орталық Азиядан Оңтүстік Азияға және оған жақын аймақтарға дейін созылады. Осы кеңею ШЫҰ аясында цифрлық экономикалық дамудың негізі ретінде стандартталған деректерді басқару архитектурасын құрудың қажеттілігін айқындайды. Мүше мемлекеттердің әртүрлі реттеу тәсілдері мен жеткіліксіз көпжақты үйлестіру механизмдерімен сипатталатын қазіргі жағдай шұғыл институционалдық жаңартуларды талап етеді. Осы ынтымақтастық режимін орнату үшін үш негізгі баған анықталды: шекаралар аралық деректерді басқару протоколдарын әзірлеу; көпдеңгейлі заңнамалық үйлестіру құрылымдарын құру; кешенді ынтымақтастық қауіпсіздік стандарттарын енгізу. Қытайдың цифрлық трансформациядағы айқын рөлін ескере отырып, ол көпжақты платформалар арқылы өз стратегиялық жоспарын белсенді түрде алға жылжытып, ШЫҰ келіссөздерінде инновациялық шешімдерді ұсынуы және барлық мүдделі тараптарға пайда әкелетін ортақ қауіпсіздік парадигмаларын қалыптастыруы қажет.

Тірек сөздер: ШЫҰ, деректер қауіпсіздігі бойынша ынтымақтастық, деректер гегемониясы, цифрлық экономика, халықаралық ұйымдар.