Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

IRSTI 10.87.79
Scientific article

https://www.doi.org/10.32523/2616-6844-2025-150-1-219-227

Legal Aspects of Data Security Cooperation in the Development of Digital Economy of the Shanghai Cooperation Organization Member States

Zh.T. Sairambaeva[1], Zhang Ju*[1]

[1]*al-Farabi Kazakh National University*

(e-mail: [1]zhuldyz.sairam@gmail.com, [2]zhangju@hrbipe.edu.cn)

Abstract: Digital economy cooperation has become an emerging area of cooperation for the SCO. However, data security issues such as data leakage and cross-border data flow risk have been highlighted. The fundamental reason is that there are obvious differences in data security laws and the lack of a legal mechanism for data security cooperation. Therefore, according to the characteristics of the SCO member states, the basic principles and the idea of a legal mechanism. These legal mechanism ideas include a win-win cooperation data security concept, a data security cooperation platform, digital products, and a digital services supply chain security legal framework system to protect the citizens of personal data security legal mechanism and form a "good data protection" and "data development and utilization" system environment. At the same time, these mechanisms must provide data subjects between "data resources and data assets" "sharing, reciprocity, trading, and exchange" activities of data security cooperation system compatibility. The legal mechanisms of data security cooperation in the SCO digital economy cooperation should be a sustainable development and dynamic legal mechanism.

Keywords: Shanghai Cooperation Organization, digital economy cooperation, legal aspects of data security cooperation.

Received: 21.01.2025. Accepted: 10.03.2025. Available online: 30.03.2025.

Introduction

The SCO has gradually improved its organizational structure and legal framework agreements. For example, in 2019, the Kazakh government formulated and adopted the Roadmap for the Development of E-commerce until 2025. In June 2020, Kazakh President Kassym-Jomart Tokayev signed the Bill on the Amendment and Supplement to the Law on the Management of Digital Technology. This legislation, which included 35 amendments, revised the information law and introduced numerous new terms, such as chain blocks, distributed data platforms, data analysis, intelligent robots, Kazakhstan Internet space, digital assets, digital document services, digital mining, and digital tokens. In October 2020, the Kazakh government revised the National Plan for Digital Kazakhstan, defining 10 priority development directions, including the development of digital tools for public security. According to the international experience, the basic ways, and goals of developing the domestic relevant industries are put forward. In 2023-2024, Kazakhstan is developing the Digital Code. The Code covers three main areas: digital human rights and civil rights, digital economy, and digital state. The goal is to create a secure, accessible, and comfortable digital environment that provides high-tech, reliable, accessible, and secure information communication. A series of legal mechanisms have been formed. However, with the continuous expansion and upgrading of cooperation areas, data security issues such as data leakage and cross-border data flow risks have also become prominent. Therefore, in the era of big data, using legal mechanisms to ensure data security is the requirement of regulating the development of the SCO's digital economy. Without data security, the SCO cannot achieve digital economy cooperation.

Research methods

This article uses the historical analysis, literature analysis, and comparative legal analysis method through the analysis of the Shanghai economic cooperation in the process of data security legal documents, comparing the differences and the legal system from the perspective of international law conception of the SCO legal mechanisms, promoting the digital economic cooperation and the development of data security.

This article analyzes a series of important documents on the economic cooperation of the SCO, including the National Plan for Digital Kazakhstan, the Cyber Security Law, and the National Cyberspace Security Strategy successively issued by China in recent years. At present, the research on SCO economic cooperation, especially digital economy cooperation, mainly focuses on two aspects. The first is the development status of the digital economy infrastructure. Second, to review and discuss the impact of data security legal regulations on the SCO digital economy cooperation, to provide reference and basis for this study. On this basis, to find more effective legal ways to improve data security.

Discussion and results

The necessity of the legal construction of the SCO data security cooperation.

The development of the digital economy has become the key to global development and competition. For example, the Kazakh government formulated a digital Kazakhstan, and the

Chinese government issued a different digital economy development plan [1]. For instance, during the first China-Central Asia Summit in May 2023, Huawei Kazakhstan Company and Kazakhstan National Railway Company signed a partnership agreement to build smart and digital railways. In February 2024, the Joint Innovation Center of Huawei-Kazakhstan National Railway Company was officially established in Astana, the capital of Kazakhstan. Kazakh President Tokayev unveiled the center and delivered a speech. The Joint Innovation Center will rely on Huawei's advanced technologies and solutions in artificial intelligence, cloud, LTE, and other fields to help Kazakhstan build an efficient, safe, personalized, and intelligent railway system. The above cooperation in the field of the digital economy of the SCO member states requires legal mechanisms to ensure their data security. However, the current legal mechanism does not fully guarantee the data security of the SCO member states in the development of the digital economy.

There is a big gap between the data security laws of the SCO member states and the developed countries in the world. The members of the SCO have recognized the strategic value behind these data resources. At the same time, the data security rule of law among the member states has been elevated to the level of "national security" and "national competitiveness". For example, China has promoted the construction of a new legal relationship for data security and actively participated in the reform and construction of the global data security governance system. Kazakhstan has improved the domestic data security legislation, established a data security legal system, prevented the data system from being attacked and threatened, improved the national data security guarantee capability, and established a data security emergency mechanism. Despite the numerous efforts of the member states, there is still a gap with the developed countries [2].

The SCO lacks a unified and applicable data security legal system in economic cooperation. Data security has been recognized and concerned in the process of the economic cooperation of the SCO, but there is no unified legal system to regulate and restrict the data security of the SCO. This is an important issue that deserves both attention and research. At present, multi-domain and multi-dimensional SCO data security involves the inconsistency of the needs of multiple data subjects, which also leads to the fragmentation and lack of legal supervision and supervision in the development of data security rules. The SCO data security involves the subject of, diversity and the demands of members, making the SCO members data security regulation difficult to reach a consensus on. It is difficult to form data security cooperation will, which led to the development of the SCO data security governance data security rules fragmentation and lack of legal regulation, etc. In addition, many countries employ data localization measures as the primary means of data security, with each member implementing distinct legal regulations governing cross-border data flow and localized storage data security. This leads to a lack of unified data security legal regulation across the region, resulting in a more distinct global data security legal system. The efficacy of data security measures is ambiguous, and the global data flow is restricted, which consequently leads to the stagnation of global data security legal regulations. Therefore, this reflects the complexity of the SCO data security legal regulation.

The SCO rules and regulations for data security cooperation are missing. The data security cooperation is limited to initiatives and statements, and there are no binding legal rules and

institutions, let alone relevant cooperative operating platforms. Because the SCO does not have a legal system for data security cooperation, it lacks strict constraints on cooperation. There are no data-secure communication channels between Member States, cooperation initiatives are loose, and there are no rules for implementation. At the same time, there is no platform for unified action. In the absence of the data security cooperation platform of the SCO, the consensus on data security cooperation only stays in the statement and appeal and cannot be implemented in the system construction of action constraints.

Data security cooperation is not deep enough. The development history of the SCO has a short economy. In recent years, cross-border e-commerce trade between China and Kazakhstan, as well as digital communication, warehousing and logistics, information communication, and digital construction, have become new highlights of bilateral economic and trade cooperation. In October 2022, Huawei Technology, the Kazakhstan company, and the digital development, innovation, and aerospace industry signed a memorandum of understanding to create a digital center and open the digital economy in the field of cooperation. The main areas of cooperation are in the communication infrastructure development that introduced advanced digital solutions, broadband Internet, mobile Internet, and 5G project. The legal guarantee of data security still needs to be explored and developed gradually in practice.

In order to address the above issues, we need to establish a legal mechanism for data security cooperation in the development of the SCO digital economy. Here are some fundamental principles for building this data security legal mechanism within SCO framework.

Data security is an important area to ensure the development of the SCO's digital economy. Its basic principles should include the principles of data sovereignty, security development, fairness and justice, and cooperation.

This is the core principle of the legal mechanism of the SCO for data security cooperation. Data security is the key strategic resource guarantee of modern countries, and it is related to human security, national security, and social stability. Having the generation, utilization, processing, management, security, and exchange of any data within the sovereign jurisdiction, as well as the decision of data procedures and methods to participate in international data activities, to protect its data security and avoid the data rights and interests of any country, which is an important part of ensuring national data security.

The principle of security development is an important principle to be followed in the construction of the SCO data security legal mechanism; that is, countries should seek the development of a digital economy while strengthening the protection of data security. The principle requires the SCO to adopt laws to protect the data security of the countries, enterprises, and individuals of its member states and not to harm the national data security of any member state. To provide security protection for the digital services of the SCO enterprises.

The SCO member states follow the basic spirit of fairness, mutual benefit, win-win cooperation, and equal development. All the member states should achieve the goal of common development. The SCO member states advocate data security multilateralism and respect data sovereignty, and the status of the member states should be equal, not privileged, big, or small.

The SCO data security cooperation is a key factor. In the construction of the data security legal mechanism, the SCO should strengthen data security cooperation, seek common data

development, and jointly promote the construction of the SCO data security cooperation platform and legal mechanism that meets the requirements of member states and does not violate the data interests of member states.

The SCO Data Security Cooperation Committee has been established. Staff members will meet and establish the corresponding organizational structure. The security data concession agreement connects the institutions and rules of data security and stability and establishes the consultation and decision-making mechanism, supervision mechanism, and dispute resolution mechanism of the data security platform. Sub-committees include Trade Data Security Committee, Investment Data Security Committee, Financial Data Security Cooperation Committee, Intellectual Property Data Security Committee, etc. Through the data security platform, supervise, use, and protect the security of all kinds of data, and sign the data security agreement through the platform to ensure that the data security has a legal basis. The SCO data security cooperation platform can carry out data security law enforcement cooperation, crack down on and prevent data security crimes, and promote data security in the economic cooperation [3]. The data security platform is also the basis of sharing the future network community. The SCO data security platform can cooperate with the data security law enforcement. In November 2020, the SCO member states called on the international community to strengthen cooperation in the digital economy and jointly build a community that shares the future in cyberspace, including preventing disputes caused by data security, ensuring economic development, and improving people's livelihoods [4].

Digital products and digital service supply chains are a kind of network structure that links the demand side and the supply side in the process of digital data resources and data services. The data products and data services provided to the demand side are the supply chain links connecting the supplier and the demand side in each link of the data products and data services, including production, use, and circulation. If there are supply chain problems such as security loopholes and security defects, the whole order of the supply chain will be affected, and even both the supply side and the demand side may suffer losses. Therefore, there needs to be a stable, open, and secure data-running environment for the digital products and data services supply chain.

Legally collected and used citizens' names, genders, ID card numbers and other information related to individual citizens, that is, citizens' personal information. Information that a citizen does not wish to disclose or shall not be disclosed without the consent of the individual. This is the personal privacy of the citizens. At present, the personal information and privacy on the SCO Internet are facing the risk of leakage, theft, and tampering. To protect the data security and privacy rights of citizens in the SCO member states, efforts must be made at the technical, organizational, and legal levels to innovate and build safeguards [5].

The SCO Data Security Cooperation Organization performs its duties as a data security-related agreement. The function of the organization is to establish the basic principles, legal system, and operation mechanism of SCO data security cooperation through negotiations to help its member states better formulate legal systems related to data security. The domestic data security legal systems of all members promote the establishment of formal and informal

review exchanges through SCO data security organization activities, such as regular meetings and policy reviews. The SCO data security cooperation initiative should be implemented in the construction of legal mechanisms. The SCO Data Security Cooperation Organization and its legal mechanisms include data security rules and institutions and establish a legal system related to data security.

The dispute settlement mechanism of the SCO data security cooperation is to handle peaceful disputes over data security in the process of data generation, application, circulation, and exchange of data in the SCO digital economy cooperation. Dispute settlement experts should be selected from the members of the SCO data security expert group, and the SCO data security disputes should be under the jurisdiction of the agency. The SCO Data Security Cooperation Organization Agreement authorizes the jurisdiction of the SCO body, and its data security entity rules and procedural rules are established through the rules of the SCO Data Security Dispute Settlement Mechanism. The data security dispute of the SCO shall first be settled through negotiation and consultation. If an agreement cannot be reached, it shall be conducted through the agency [6].

Conclusions

On July 2, 2024, the Chinese President Xi Jinping arrived in Astana attend the Shanghai Cooperation Organization summit. In Kazakhstanskaya Pravda and the Kazakh international news agency published and signed an article titled "Concentric Written China-Kazakhstan Relations New Chapter". The article stated that China is willing to work with "fair Kazakhstan" economic policy, deepen economic and trade cooperation, fully explore the potential digital economy collaboration, and add more new momentum for cooperation between the two countries. It is the proper meaning of the big data era to make reasonable legal regulation on the data security development in the SCO digital economy cooperation. Based on the SCO's consensus on developing a digital economy and information security cooperation and the experience of innovation cooperation in countries developed in digital information technology, the SCO needs to achieve synergy in legal mechanisms. Specific measures include the principle of data sovereignty, security and development, and the concept of a digital economy featuring win-win cooperation in accordance with the principle of fairness and justice. Establish the Shanghai Cooperation Organization data security cooperation platform, establish a digital products and digital services supply chain security legal framework system, and create the protection of citizens' personal data security and privacy. The SCO data security cooperation dispute settlement mechanism and establish the SCO digital economic cooperation committee set up the data security cooperation working group to ensure the data security has a stable working mechanism. The best legal mechanism for data security in the SCO digital economy cooperation should maintain a balance between data security and data availability, effectively connect the laws and regulations related to data security of member states in digital economy cooperation and be a legal mechanism for sustainable development.

Contribution of the authors

The authors contribute equally. **Zhang Ju** completed the collection and collation of the preliminary data and wrote the first draft of the article. **Zh.T. Sairambaeva,** on this basis, a critical review, made many suggestions and opinions and further guided the completion of the final article, especially in the conclusion section.

References

1. Liu Huaqin. (2016) «Promote a new space for SCO regional economic cooperation with digital economy », Russian Academic Journal, Vol-12(3) , pp. 5-24. Available at: https://kns.cnki.net/kcms2/article/abstract?v=RkYMyaebi8VdXJ47717eXuEzwIrAFDNB4IRY6C2eV2I8isb-CZOfT97eUEzGJ_tiE5WIee6Uud7k0hVPHHTHDyQa3QeEoLGIAXn1B09lUO2ZGAWnSRRNQ0STT7LF1nXlqjkF8tHdoWk=&uniplatform=NZKPT&language=CHS. (accessed: 12. 07. 2024).

2. Chen Yongmei, Guo Shufang. (2023) «The Construction of the SCO data Security Cooperation Legal Mechanism », Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition), Vol-44(12), pp. 59-65. Available at: https://kns.cnki.net/kcms2/article/abstract?v=m22VhQxdXydgvgkvVJ8d0QpFs7FEzif6NmC1IglJn0Jh_7FyQHsOPc8ZwQVof1eS0IVrSi9_gnMRF4RSNP5wX9EPafbL1V8fhAhjxhtuwJZbW9i0qvzdC0GJbTC1kyB-axCExoyKR9IuPfqK2Zsokg==&uniplatform=NZKPT&language=CHS. (accessed: 14.07. 2024).

3. «Statement of the Council of Heads of State of the Shanghai Cooperation Organization on safeguarding cooperation in the field of international information security, 2020.11.10)». Available at: https://chn.sectsco.org/20201110/689647.html. (accessed: 20.08. 2024).

4. Xiao Bin. (2021) «Developing the SCO Digital Economy: Based on the perspective of data security cooperation», China Information Security, Vol-44(8), pp. 81-82. Available at: https://kns.cnki.net/kcms2/article/abstract?v=RkYMyaebi8Vb9bfGSuPpZp_KkMf3pkTH2S4jO9N-yKUqdAPv_eoX52SZg8Qr9_Ip0nftIoHW7kNI2Js3gp9ERxtDi09ZyroFcr0OCclUmAZ_ZkKlFtPAUZL8RhI6Pr7-5DHf0CMyDv8=&uniplatform=NZKPT&language=CHS. (accessed: 22.08. 2024).

5. Wang Haiyan. (2021) «Mechanism construction and challenges of SCO information security cooperation », Information Security in China, Vol-44(8), pp. 77-80. Available at: https://kns.cnki.net/kcms2/article/abstract?v=RkYMyaebi8Ur4oL2u9FI_6WkzGDjVZdwrQ6ZSqK9jNBNDnvxbzqTRRHoPFvRzx_P0J9r2MnFyGttAmS7UA3pO7hVQEc7aU8Z2oOycTtz3D2FQhgE8rTeyAEX6mFGfq8k7yRksgCCsGw=&uniplatform=NZKPT&language=CHS77-80. (accessed: 22.09.2024).

6. Yue Shumei. (2021) «Research on the construction of international cooperation legal mechanism for civil Nuclear Energy Safety guarantee », Wuhan Review of International Law, Vol-1(4), pp. 1-17. Available at: https://kns.cnki.net/kcms2/article/abstract?v=RkYMyaebi8VIplo0SWxo4-nZeVjJ-IZjor4v5UuyfiO86d50zGMC-gyOSXhG67AxoBvapqgLl8ZDrXM5-dZ8nMfY0Mellsv3rkDMdNwCzwHkO6XeCWiMqJzLgBxx8puRm7TQ77hPIAo=&uniplatform=NZKPT&language=CHS. (accessed: 22.09.2024).

Ж.Т. Сайрамбаева[1], Джан Цзю[1]
[1]Казахский национальный университет имени аль-Фараби
(e-mail: [1]zhuldyz.sairam@gmail.com, [2]zhangju@hrbipe.edu.cn)

Правовые аспекты сотрудничества в области безопасности данных в развитии цифровой экономики государств – членов Шанхайской организации сотрудничества

Ааннотация: Как многосторонняя региональная международная организация, правовой аспект сотрудничества является важной поддержкой его существования и развития. Сотрудничество Шанхайской организации сотрудничества (ШОС) в экономической сфере углубляется и расширяется, а режим и механизм сотрудничества постепенно меняются и модернизируются. Сотрудничество в области цифровой экономики стало новой областью сотрудничества для ШОС. Однако были подчеркнуты проблемы безопасности данных, такие как утечка данных и риск трансграничного потока данных. Основная причина заключается в том, что между государствами-членами ШОС существуют очевидные различия в законодательстве и нормативных актах по безопасности данных, а также в отсутствии правового механизма сотрудничества в области безопасности данных. Поэтому, в соответствии с особенностями государств-членов ШОС, основными принципами и идеей правового механизма. Эти идеи правового механизма, включая концепцию безопасности данных взаимовыгодного сотрудничества, платформу сотрудничества в области безопасности данных, систему правовых рамок безопасности цепочки поставок цифровых продуктов и цифровых услуг, защиту граждан правового механизма безопасности персональных данных, формирование системной среды "хорошей защиты данных" и "разработки и использования данных", в то же время необходимо обеспечить субъект данных между "ресурсами данных и активами данных" "обмен, взаимность, торговля, обмен" деятельностью совместимости системы сотрудничества в области безопасности данных. Правовый механизм сотрудничества в области безопасности данных в сфере цифровой экономики должен быть устойчивым развитием и динамичным правовым механизмом.

Ключевые слова: Шанхайская организация сотрудничества, сотрудничество в области цифровой экономики, Правовые аспекты сотрудничества в области информационной безопасности.

Ж.Т. Сайрамбаева[1], Джан Цзю[1]
[1]әл-Фараби атындағы Қазақ ұлтық университеті
(e-mail: [1]zhuldyz.sairam@gmail.com, [2]zhangju@hrbipe.edu.cn)

Шанхай ынтымақтастық ұйымына мүше мемлекеттердің цифрлық экономиканы дамыту саласындағы деректер қауіпсіздігі саласындағы ынтымақтастықтың құқықтық аспектілері

Андатпа: Көпжақты өңірлік халықаралық ұйым ретінде ынтымақтастықтың құқықтық аспектісі оның өмір сүруі мен дамуы үшін маңызды қолдау болып табылады. Шанхай ынтымақтастық ұйымының (ШЫҰ) экономикалық саладағы ынтымақтастығы тереңдеп, кеңейе түсті, ынтымақтастық режимі мен тетігі біртіндеп өзгеріп келеді және жаңарту. Цифрлық

экономика саласындағы ынтымақтастық ШЫҰ үшін ынтымақтастықтың қалыптасып келе жатқан саласына айналды. Сонымен қатар, деректердің жылыстауы және трансшекаралық деректер ағынының тәуекелі сияқты деректер қауіпсіздігі мәселелері ерекше атап өтілді. Негізгі себеп - ШЫҰ-ға мүше мемлекеттер арасында деректердің қауіпсіздігі туралы заңдар мен ережелерде айқын айырмашылықтар болуы және деректердің қауіпсіздігі саласындағы ынтымақтастықтың құқықтық тетігінің жоқтығы. Сондықтан ШЫҰ-ға мүше мемлекеттердің ерекшеліктеріне сәйкес, негізгі қағидаттар мен құқықтық тетік идеясы. Бұл құқықтық тетік идеялары, оның ішінде ұтыс кооперациясының деректер қауіпсіздігі тұжырымдамасы, деректер қауіпсіздігі саласындағы ынтымақтастық платформасы, цифрлық өнімдер және цифрлық қызметтер жеткізу тізбегінің қауіпсіздікті қамтамасыз етудің құқықтық базасының жүйесі, дербес деректер қауіпсіздігінің құқықтық тетігінің азаматтарын қорғау, «деректерді жақсы қорғау» және «деректерді әзірлеу және пайдалану» жүйелік ортасын қалыптастыру, сонымен бірге «деректер ресурстары мен деректер активтері» арасындағы деректер субъектісін қамтамасыз ету қажет. өзаралық, сауда, биржалық" деректер қауіпсіздігі саласындағы ынтымақтастық жүйесінің үйлесімділік қызметі. ШЫҰ цифрлық экономика саласындағы ынтымақтастықта деректер қауіпсіздігі саласындағы ынтымақтастықтың құқықтық тетігі орнықты даму және серпінді дамып келе жатқан құқықтық тетік болуы тиіс.

Түйінді сөздер: Шанхай ынтымақтастық ұйымы, цифрлық экономика саласындағы ынтымақтастық, деректер қауіпсіздігі саласындағы ынтымақтастықтың құқықтық аспектілері.

Information about the authors:

Сайрамбаева Ж.Т. **–** з.ғ.к., халықаралық құқық кафедрасының доценті, әл-Фараби атындағы Қазақ ұлттық университеті, Қарасай батыр көш., 95 А, Алматы, Қазақстан

Чжан Цзю **–** хат-хабар авторы, магистр, халықаралық құқық кафедрасының докторанты, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қарасай батыр көш., 95 А, Алматы, Қазақстан

Сайрамбаева Ж.Т. **–** к.ю.н., доцент кафедры международного права, Казахский национальный университет имени аль-Фараби, ул. Карасай батыра, 95А, Алматы, Казахстан

Чжан Цзю **–** автор для корреспонденции, магистр, докторант кафедры международного права, Казахский национальный университет имени аль-Фараби, ул. Карасай батыра, 95А, Алматы, Казахстан

Sairambaeva Zh. **–** PhD in Law, Associate Professor, Department of International Law, Al-Farabi Kazakh National University, Karasay Batyr str., 95A, Almaty, Kazakhstan

Zhang Ju – corresponding author, master, doctoral student, Department of International Law, al-Farabi Kazakh National University, Karasay Batyr str., 95A, Almaty, Kazakhstan