Legal Guarantee Mechanism of Data Security in the Digital Economic Sector of Data Security in Digital Economy-Quaternary Cypress

Jingbai Ji*

Department of International Economics and Trade, Pearl River College, Tianjin University of Finance and Economics, Tianjin, 301800, China

*Jib20050529@outlook.com

Abstract. With the vigorous development of the digital economy, data has become a core production factor driving economic growth and social progress. However, the extensive collection, storage and use of data have also brought numerous security challenges, such as data leakage, abuse, and risks associated with cross-border flows. These risks not only threaten personal privacy and corporate interests but also concern national economic security and social stability. Against this backdrop, it is particularly urgent to establish a complete legal guarantee mechanism for data security in the digital economy. This article, through an in-depth analysis of the risks and challenges faced by data security in the era of the digital economy, explores the current situation and deficiencies of the existing data security legal guarantee mechanism in China. The research finds that although China has initially established a data security legal system, there are still many problems in the refinement of laws, their enforcement, and coordination with other laws. Therefore, this article puts forward targeted improvement suggestions, including further refining data security laws and regulations, clarifying data ownership and responsibility subjects, strengthening the regulatory mechanism for cross-border data flows, and introducing new technological means to enhance data security guarantee capabilities. Through these measures, the aim is to provide a solid legal guarantee for the high-quality development of the digital economy, promote the maximization of data value within a safe and compliant framework, and facilitate the sustainable growth trajectory of the digital economy.

Keywords: Data security; Digital economy; Security; Legal issues; Suggestions for improvement

1 Introduction

With the vigorous development of the digital economy, data has become a key factor of production, and its security is directly related to personal privacy, enterprise competitiveness and even national security. However, the rapid circulation and wide application of data has also brought many security risks, such as data leakage, abuse, etc. It

© The Author(s) 2025

B. Siuta-Tokarska et al. (eds.), *Proceedings of the 2025 3rd International Academic Conference on Management Innovation and Economic Development (MIED 2025)*, Advances in Economics, Business and Management Research 348,
https://doi.org/10.2991/978-94-6463-835-6_59

is urgent to improve the legal protection mechanism to regulate and restrict. This paper aims to deeply explore the legal guarantee mechanism of data security in the digital economy, analyze the deficiencies of the current legal framework, and put forward targeted suggestions for improvement, in order to provide solid legal support for the thriving and sustainable expansion of the digital economy and promote the value maximization of data on the track of security and compliance.

2 Definition of Digital Economy

Digital economy refers to a series of economic activities that take data resources as key factors of production, modern information networks as an important carrier, and the effective use of information and communication technology as an important driving force for efficiency improvement and economic structure optimization. The digital economy is the main economic form after the agricultural economy and industrial economy. The digital economy covers two aspects of digital industrialization and industrial digitalization. Digital industrialization includes digital product manufacturing, digital product service industry and digital technology application industry, which is the basis for the development of digital economy; Industrial digitalization refers to the traditional industries through the introduction of digital technology to achieve the digital transformation of production mode, management mode and service mode. The digital economy is characterized by networking, intelligence and individuation. It can break the constraints of time and space, reduce transaction costs, expand market boundaries, and realize efficient and accurate resource allocation.

3 Definition of Data Security

Data security means to ensure the integrity, confidentiality and availability of data by taking necessary measures to ensure that data is not released without authorization, leaked, tampered with, destroyed or illegally used during storage, transmission and processing. The three core elements of data security are: 1. Confidentiality: to ensure that data can only be accessed and used by authorized users, and to prevent data leakage or illegal access; 2: Integrity: ensure that the data is not tampered with or damaged in the process of storage, transmission and processing to ensure the accuracy and reliability of the data; 3: availability: to ensure that the data can be accessed and used by authorized users in a timely and reliable manner when needed to avoid data loss and unavailability. Data security involves individuals, enterprises, governments and other levels, covering everything from the protection of personal privacy to the security of the nation's critical information infrastructure. Data security is a systematic project that requires coordinated protection from many aspects, including technology, management and law.

4 The Problem of Data Security in Digital Economy

4.1 Connotation of Data Security Issues

"Data security means taking the necessary measures to ensure that data is in a state of effective protection and lawful use, as well as having the ability to guarantee a state of continuous security. Data security becomes an important part of national security [1]." This shows that the connotation of data is no longer limited to the protection of personal information, but is closely linked to national security as an important resource element. At present, countries have a deepening understanding of data security, and have clarified the strategic position of data through policy or legal means. For example, the United Kingdom of Great Britain and Northern Ireland government has published its National Data Strategy, which sets out a path to realize the value of data and points out the direction for promoting data growth, building trustworthy data mechanisms, and ensuring the security and resilience of data infrastructure, so as to ensure national security. Judging from the current legislative trend, countries will further improve data security standards, laws and regulations and strategic planning from a national perspective and explore the balance between the development of digital trade, data security and national security.

4.2 Development Stages of Data Security Issues

Under the wave of continuous iteration and upgrading of global technology, people's awareness of data security continues to deepen. The development process of data security can be roughly divided into three stages. In the first stage, the core goal of data security is to protect the database system, and its main idea is to ensure the security of the database based on the concept of system security. The focus of this stage is to prevent external intrusion into the database, while strengthening the security of the internal system, and carry out effective supervision of external behavior. It can be seen that the data security work in this stage mainly focuses on "database security". Entering the second stage, the focus of data security has shifted, focusing on the security of data leaving the database, when the data user uses the data, and when the data flows to the third-party service platform. This stage takes "data scenarioization" as the core, emphasizing the need to preset data to specific use scenarios for in-depth discussion, and requires the security governance provided by third-party platforms to meet the needs of specific activity scenarios. In the third stage, the core of data security is transformed into "data security governance". Through the superposition of technology integration and organizational norms, the overall data security situation is presented. As data is promoted to the level of national assets and critical infrastructure, data security is no longer just a technical level of security, but has evolved into a systematic security, which has become the most important feature of this stage [2]. At present, China has entered the third stage with "data security governance" as the core. In the context of digital security governance, significant changes have taken place in the policy environment, market environment and development model of digital trade. On the one hand,

laws, regulations and policies related to data security governance have been continuously introduced and improved; On the other hand, enterprises involved in international trade are also facing a series of rectification and interviews to ensure their compliance in data security.

4.3 Data Security Risks Have Risen Sharply

Digital technologies promote the diversification of participants, data flow platforms and data application scenarios, and data security risks are rising sharply. In the context of the accelerated global digitization process, the field of data security is facing a variety of severe challenges, of which several typical data risks are particularly prominent: First, data trafficking. The core of the digital economy is to deeply explore the potential value of personal information and cutting-edge information technology. With the rapid development of information technology, the importance of personal data becomes more and more prominent. The identification attributes contained in personal data may be used by criminals and become a tool to attack personal privacy and rights. At present, data trafficking has become a gray area that is hard to ignore in the big data industry. Some criminals collect and trade personal data through illegal channels, seriously violating users' privacy and information security, and bringing many potential risks to individuals and society. Second, data monopoly. The lawful and compliant collection and use of data is the basis for ensuring data security. However, due to the asymmetry in information acquisition and resource control between individuals, enterprises and institutions, the lawful and compliant collection of data often depends on the self-discipline of enterprises and institutions. Once personal data flows into the platform, the individual's control over the data is weakened and the platform becomes dominant. This asymmetrical data power pattern leads to frequent data monopolies. Data monopoly not only leads to the abuse of digital rights, but also may cause damage to the market competition order and even threaten national security. For example, some large Internet platforms, with their huge resources of user data, have formed monopolies that limit the fair circulation and innovative application of data. Third, data theft. The illegal theft of data has been going on for a long time, and with the rapid development of information technology, its means are becoming more complex and covert. Criminals use advanced technical means, such as hacker attacks, malware implantation, etc., to invade websites, servers and other data sources and obtain a large amount of sensitive information. In recent years, the wide application of "crawler" technology has provided a new opportunity for data theft. By writing malicious crawler programs, some lawbreakers bypass the security protection measures of websites and grab user data in batches, bringing huge security risks to enterprises and individuals. Data theft will not only lead to the disclosure of personal privacy, but also may cause the disclosure of business secrets of enterprises, and even affect the national information security. Fourth, data leakage. The risk of data leakage has gradually expanded from the individual and enterprise level to the entire industry, and even threatens national security [3]. At present, the popularity of science and technology and the Internet has made various apps, web pages and small programs embedded in applications widely used. While providing convenient services, these platforms also require users to authorize access to a large amount of personal

information, such as location, identity and contact information. Excessive requests for access to and acquisition of user data not only increase the risk of exposing user privacy, but also provide opportunities for criminals. Once the data is leaked, it will not only bring problems such as fraud and harassment to individuals, but also may trigger a crisis of trust in enterprises, and even pose a threat to the healthy development of the entire industry and the country's digital security. To sum up, data trafficking, data monopoly, data theft and data leakage are several typical risks facing the current global data security field, which not only pose a threat to personal privacy and rights, but also may have a serious impact on the business interests of enterprises, the stable development of the industry and the security and stability of the country.

5 Legal Protection Mechanism

5.1 The Data Security Law Addresses Data Security Issues in Various Ways

Emphasize the Balance Between Data Security and Development. The introduction of the Data Security Law provides a solid legal basis for effective data supervision and governance, and fills the gap in China's data security protection legislation. At the same time, the law not only focuses on the security of data, but also actively encourages the rational and efficient use of data according to law, and advocates a sound balance between data security and application development through technological innovation and business model innovation. In the second chapter of the Data Security Law, the principle of parallel data security and development is clearly explained, and the relationship between "data security" and "data utilization" is further clarified. According to the Law, the state, as the core body coordinating data security and development (Article 13), adopts a series of specific measures to ensure that data security and development go hand in hand. The specific measures and regulations are shown in Table 1.

Table 1. Specific measures and relevant regulations [4]

Measures	Ordinances
Advancing data infrastructure	Article 14
Raise the level of intelligence in public services	Article 15
To support the utilization and enhancement of data and research on data security technologies	Article 16
Promote the construction of data security management standard system	Article 17
To promote the development of services such as data security testing, evaluation and certification	Article 18
Establish and improve the data transaction management system	Article 19
Support technical and training education related to data security	Article 20

Through the above-mentioned measures, the State has given full play to its leading role in the construction of key data systems, improved the supporting measures for the development of industries related to data security and the exploitation and utilization

of data, and achieved the strategic goal of promoting security through development and ensuring development through security.

Stipulate Regulatory Requirements for Cross-border Data Flows. In today's digital age, cross-border data flows are becoming increasingly frequent and a regular phenomenon. However, the cross-border flow of data often involves key issues such as cyberspace sovereignty, data sovereignty and data security, so it has always been an area that countries focus on in the process of data legislation. In response to the challenges posed by cross-border data flows, countries have implemented data export controls and taken counter-sanctions measures. In terms of cross-border data flows, the Data Security Law does not take the extreme approach of a total ban, but only makes framework institutional arrangements for key areas such as data of Items subject to national security restrictions controlled items related to national security and important data leaving the country, aiming to ensure that data can flow across borders in an orderly and free manner Conforming to legal standards. The law further clarifies the regulatory requirements in cross-border data flows, and safeguards the country's data sovereignty through corresponding system design [5]. Specifically, on the one hand, the Data Security Law clarifies that safeguarding National security and benefits and fulfilling International duties and responsibilities can be the legal basis for prohibiting the export of relevant data; On the other hand, it also clarifies the legislative position that China has the right to take reciprocal countermeasures against foreign investment and trade discrimination in the field of data. These regulations fully reflect China's firm advocacy of data sovereignty in the cyber data space, highlighting China's awareness of sovereignty and the rule of law concept in the governance of cross-border data flows.

5.2 Electronic Commerce Law of the People's Republic of China

Provides Guarantee for the Healthy Development of E-commerce. E-commerce has become one of the core driving forces to promote the current social and economic growth. With the continuous E-commerce development and innovation industry, in order to maintain its good growth trend, it is not only limited to the richness of commodity types and the convenience of shopping experience, but also needs to provide more comprehensive protection for consumers and merchants from the legal level. The promulgation and implementation of the E-commerce Law is an important legal means to ensure the healthy E-commerce advancement and Ensure the rights and interests of consumers. The implementation of the E-commerce Law is of vital significance to the standardized development of the e-commerce industry. Through clear legislative provisions, the law can effectively regulate e-commerce behaviors, maintain market order, reduce the occurrence of bad behaviors such as selling fake goods, selling fake goods, fraud and brushing orders in e-commerce platforms, so as to greatly protect the rights and interests of consumers and create a good e-commerce operating environment. In such an environment, consumers will have more confidence in the orderly development of the e-commerce market, and e-commerce operators will be able to obtain a broader space for development [6]. As a norm of market conduct, the E-commerce Law not only promotes the behavior of buyers and sellers to be more standardized, but also provides a legal basis for the regulatory authorities to implement convenient supervision

over market entities. According to the law, the regulatory authorities can guide e-commerce enterprises to apply for business licenses more effectively and ensure their legal and compliant operations. In addition, the E-commerce Law also provides guidance and guarantee for local economic development through e-commerce platforms, effectively promoting the deep integration of e-commerce and the real economy. At the same time, the E-commerce Law encourages the innovative and green development of e-commerce, especially in emerging areas such as rural e-commerce and cross-border e-commerce, which can provide strong legal support. This enables localities to use e-commerce platforms to serve local economic development in accordance with local conditions, and boost the healthy and well - regulated development of rural e-commerce and cross-border e-commerce.

Safeguarding and Protecting Consumers' Rights and Interests. The key reason why e-commerce can achieve rapid development is that it breaks through many limitations of traditional business models. It transcends the geographical restrictions and can accurately meet the personalized and diversified needs of different consumers, which is difficult for traditional business models to achieve in terms of flexibility and convenience. However, it is precisely because of the particularity of e-commerce operation that there are also some behaviors that harm the interests of consumers in the development process, such as fraud, commodity quality problems, consumer personal information leakage and payment security problems. The existence of these problems not only affects the shopping experience of consumers, but also poses a potential threat to the healthy development of the entire e-commerce industry. The promulgation and implementation of the E-commerce Law has provided a strong legal basis for standardizing the behavior of merchants and cracking down on improper marketing methods, thus safeguarding the rights and interests of consumers and safeguarding the public interests of society.

The implementation of "E-commerce Law", its standard requirements can effectively curb the false advertising behavior of merchants. For example, the law clearly prohibits e-commerce operators from conducting false or misleading publicity through fictitious transactions and fabricating user evaluations. This regulation can effectively prevent consumers from being misled by false information, thus effectively protecting the legitimate rights and interests of consumers. At the same time, the law also puts forward strict requirements on platform operators in terms of product information disclosure, prohibiting them from exaggerating the functions and functions of goods or misleading consumers through virtual publicity. By restoring the product functions themselves, the law helps consumers avoid making unwise consumption decisions based on false information. In addition, the E-commerce Law fully protects consumers' right to evaluate products. For those products with exaggerated or false publicity, consumers can send warnings to other consumers by way of comments, or express their real consumption experience of the products through comments. Different comments can play a corresponding role: on the one hand, it can provide important reference information for other consumers and play a warning role; On the other hand, it can also make a positive contribution in the recognition and promotion of businesses. The relevant provisions clearly stipulate that operating platforms are not allowed to delete consumers' evaluations of goods sold or services provided on their platforms. An effective

evaluation mechanism not only provides an important basis for consumers' shopping decisions, but also serves as an important driving force for operators to improve business quality.

6 The Inadequacy and Future Prospect of the Existing Law

6.1 Accelerate the Construction of Supporting Systems and Help the Implementation of the Data Security Law

As the "Data Security Law" is about to be formally implemented, it faces many key tasks in the process of implementation. On the one hand, it is necessary to accelerate the implementation of the various systems of the law; On the other hand, efforts should also be made to address the institutional linkage between the Data Security Law, the Cybersecurity Law, the Personal Information Protection Law and other relevant legislation, so as to ensure the coordination and effectiveness of the entire legal system. First of all, the Data Security Law, as a basic law, has a legislative style of "rough rather than fine", which determines that many provisions are more principled. Although this legislative method provides space for subsequent refinement, it also means that its implementation needs to rely on supporting administrative regulations, departmental rules and national standards to further clarify and refine. For example, the law puts forward important requirements such as data classification and classification protection, important data catalog management, and important data exit security management, but the specific content and implementation details of these systems are not specified in detail in the law. This may lead to various types of data processors facing certain difficulties and uncertainties in fulfilling their data security protection obligations. Therefore, in the future, we should promote the formulation of relevant supporting administrative regulations and departmental rules as soon as possible, clarify the specific content and unified requirements of the above system, and provide more detailed operational guidelines for enterprise compliance through national standards and industry standards. Secondly, there is a connection problem between the many systems in the Data Security Law and the current legal system, which needs to be clarified and optimized. With the introduction of the Privacy and Data Protection Law, China has formed a parallel situation of three laws: Network Security Law, Data Security Law and Personal Information Protection Law. These three laws have certain crossover and overlap in the system design. For example, the cybersecurity review system in the Cybersecurity Law itself contains the content of reviewing data risks in products or services; In the case of the current data market elements mainly personal information, the data security incident reporting and important data exit management systems in the Data Security Law also have obvious crossover with the personal information leakage incident reporting and personal information exit systems in the Personal Information Protection Law. These problems may not only lead to the waste of regulatory resources, but also increase the compliance costs of enterprises [7]. Therefore, it is urgent for the competent authorities to clarify the applicable boundaries of these systems in a targeted manner and establish appropriate optimization mechanisms to avoid duplication and conflicts between systems and ensure the coordination and efficiency of the legal system.

6.2 The Improvement and Development Strategy of E-Commerce Legal System

Strengthen the Construction of E-commerce Laws and Regulations. The implementation of the E-commerce Law and its role should be closely combined with the actual situation and needs of the development of e-commerce, so as to meet the many challenges faced by the current implementation of the Law. The primary task of perfecting the legal system of e-commerce is to strengthen the construction of laws and regulations. First of all, we should start from the legal level to further improve the e-commerce contract system. Define the essential elements of electronic contract, and formulate corresponding laws and regulations according to these elements to standardize the signing and performance process of electronic contract, so as to ensure the fairness and legitimacy of electronic commerce contract. This not only helps to protect the rights and interests of both sides of the transaction, but also provides a solid legal foundation for the healthy development of e-commerce. Secondly, it is necessary to establish and improve the legal system of e-commerce payment in view of the frequent transactions in the middle line of e-commerce transactions. Clarify the legal provisions of electronic payment, standardize the behavior of electronic payment, and protect the legitimate rights and interests of both parties. The e-commerce payment link is a key area prone to breeding risks, and also an important factor leading to consumer distress and loss. Only by constantly improving the legal system in transaction payment can the rights and interests of both buyers and sellers be better protected and the healthy development of e-commerce transactions be promoted. Finally, it is necessary to further improve the protection system of e-commerce consumers' rights and interests. With the continuous development of e-commerce, new forms of transactions are emerging [8]. The traditional mode of trading through e-commerce platforms is gradually changing to private transactions. For example, new forms of e-commerce that use new media platforms or personal social platforms for online transactions are emerging. In this new form of e-commerce, the E-commerce Law needs to further improve the legislation, strengthen the protection of consumer rights and interests, encourage e-commerce operators to operate in good faith, and protect the legitimate rights and interests of consumers.

Strengthen the Supervision of E-Commerce Platforms. The core goal of the effective Operationalization of the E-commerce Law is to strengthen the regulatory function and play a key role in preventing risks and preventing them from happening in the first place through effective regulatory measures, so as to nip potential illegal acts in the bud in time. In this process, the regulatory body needs to focus on strengthening the supervision and management of e-commerce platforms. Judging from the current development trend of e-commerce, relying on e-commerce platform to carry out commercial activities has become the mainstream model of the industry. Therefore, only the implementation of effective supervision of the e-commerce platform can clarify the compliance of its operation [9]. To this end, it is necessary to establish and improve the access system of e-commerce platforms, clarify the access conditions of e-commerce platforms and standardize their operating behaviors through the formulation of sound laws and regulations, so as to ensure the legitimacy and standardization of e-commerce

platforms. At the same time, it is also necessary to strengthen the daily supervision of e-commerce platforms, regulate their business behaviors, and prevent their illegal behaviors from causing damage to consumers and operators [10]. Through these measures, the order of the e-commerce market can be better maintained, the legitimate rights and interests of all parties can be protected, and the healthy and orderly development of the e-commerce industry can be promoted. All in all, the improvement and development of the E-commerce Law has a long way to go. It is necessary to combine the actual development of the industry and continuously improve the legal system of e-commerce, safeguard the authorized rights and interests of all parties involved in e-commerce transactions, and promote the constructive advancement of e-commerce industry by starting from multiple aspects such as legal and regulatory construction, supervision and social co-governance.

7 Conclusion

With the booming development of the digital economy, data has become its core production factor, and the importance of data security has become increasingly prominent. Through the in-depth study of the legal guarantee mechanism of data security in the digital economy, this paper discusses the challenges faced by the current data security and the construction and improvement path of the legal guarantee mechanism. The research finds that data security is not only related to personal privacy and corporate interests, but also an important cornerstone of national security and social stability. Therefore, establishing a sound legal guarantee mechanism for data security is of vital significance for promoting the high-quality development of the digital economy. In the process of establishing the legal guarantee mechanism, we must adhere to the principle of taking into account data protection and openness and sharing, speed up the improvement of the data basic system, and build a comprehensive legal guarantee system for data security. This includes clarifying rules on data property rights, refining rules on data circulation and trading, and strengthening the responsibility of data security management. At the same time, it is necessary to strengthen security responsibilities, clarify the governance authority and responsibilities of relevant departments, strictly implement the security protection responsibilities of data processing entities, and ensure that the whole process of data processing complies with relevant laws and regulations. In addition, the innovation of technical means is also an important support to ensure data security. By promoting innovation in data security technologies, such as the application of cutting-edge technologies such as blockchain and trusted computing, data security protection capabilities can be effectively improved. At the same time, strengthening data security awareness education and raising the awareness of data security among practitioners and the public is also an indispensable part of building a data security legal guarantee mechanism. To sum up, the data security legal guarantee mechanism in the era of digital economy is a complex and systematic project, which requires the joint efforts of the government, enterprises, technical experts and all sectors of society. By constantly improving laws and regulations, strengthening technical support, and enhancing security awareness, data security risks can be effectively dealt with, and a solid

legal guarantee can be provided for the healthy and sustainable development of the digital economy. In the future, with the further development of the digital economy, the legal guarantee mechanism for data security should also keep pace with The Times and be continuously optimized and improved to meet new challenges and needs.

References

1. China Academy of Information and Communications Technology. International Rules of Digital Trade [M]. Beijing: Law Press, 2019.
2. Liu, Y.J.: National Security Education: The exploration process of National security discipline and some problems. Jilin University Press, Jilin (2014).
3. Gao, J., Sheng, B.: Cross-border data flow and digital trade: Domestic regulation and international rules. Exploration of International Economy and Trade (6), 117 (2024).
4. Dai Yihan. Trade Digitalization and Regulatory Fragmentation: Challenges and Responses to the Governance of Cross-border Data Flows under the Framework of International Trade Regime [J]. Journal of International Economic Law, 2021(01): 1-13.
5. Yang, L., Yuan, X.G., et al.: Research on Data Security Governance. Intellectual Property Publishing House, Beijing (2020).
6. Maidinur, M.D.: The Implementation of the E-commerce Law of the People's Republic of China and the Improvement of the System. Contemporary Law Review. (14) (2024).
7. Dai, L.: On the Protection of Personal Privacy in the Context of Digital Trade. Contemporary Law (1) (2020).
8. Zhao, X.D.: Interpretation and Principle of the E-commerce Law of the People's Republic of China. People's Court Press, Beijing (2018).
9. Lou, Y.H.: Analysis on E-commerce Platform Security obligations - Focusing on Article 38 of E-commerce Law. Journal of Lingnan Normal University 43(4), 88-96 (2020).
10. Chen, Q.W., Liu, Q.Y.: Personal Information Right and Legal Protection in the Era of Big Data. Jiangxi Social Sciences (9), 189 (2017).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.