Research on the Protection of Enterprise Data Rights and Interests in the Context of the Digital Economy

Zhiyao Jiang

Anhui University of Finance and Economics, Bengbu Anhui, 233030；

Abstract: In the current era, the wave of the digital economy has swept across the globe with great momentum, becoming the core force reshaping the global economic structure and driving a new round of industrial transformation. For enterprises, data has long transcended the simple category of an information carrier and evolved into a core asset of significant economic value and strategic importance. However, in the process of the vigorous development of the digital economy, the issue of protecting enterprise data rights and interests has become increasingly prominent, serving as a critical bottleneck restricting the sustainable development of enterprises and the construction of a healthy ecosystem for the digital economy. Based on this, this paper clarifies the theoretical and practical significance of studying the protection of enterprise data rights and interests in the context of the digital economy, identifies the practical dilemmas faced in this protection, and then proposes corresponding optimization paths, with the aim of providing suggestions for relevant research.

Keywords: Digital Economy; Enterprise Data; Rights and Interests Protection

DOI:10.69979/3041-0843.25.02.013

1 Introduction

In the contemporary era, the wave of the digital economy has swept across the globe with great force, emerging as the core driving force in reshaping the global economic structure and propelling a new round of industrial transformation. For enterprises, data has long surpassed the status of a mere information carrier and has evolved into a core asset of immense economic value and strategic significance. However, amid the robust development of the digital economy, the issue of protecting enterprise data rights and interests has become increasingly prominent, acting as a critical bottleneck that constrains the sustainable development of enterprises and the construction of a healthy ecosystem for the digital economy.From a legal perspective, the determination of data property rights ownership globally is still in a vague area. There are significant disparities among different countries and regions in terms of data legislation concepts and institutional designs, lacking a unified and authoritative legal framework for the protection of data rights and interests. Throughout the entire lifecycle of enterprise data, including collection, storage, use, sharing, and transfer, enterprises encounter numerous legal uncertainties. Data ownership disputes occur frequently, making it difficult for enterprise data rights and interests to receive adequate and effective legal protection.Against this backdrop, conducting in-depth research on the protection of enterprise data rights and interests in the context of the digital economy and exploring the establishment of a scientific, reasonable, and effective data rights and interests protection system have become urgent needs. This is essential for safeguarding the legitimate rights and interests of enterprises, stimulating their innovative vitality, and ensuring the healthy and orderly development of the digital economy. It also holds significant and far-reaching practical implications for promoting the digital transformation of the economy and society and enhancing the country's overall competitiveness.

2 Research Significance

2.1 Theoretical Significance

Firstly, it is conducive to clarifying the legal attributes of enterprise data. The definition of the legal attributes of enterprise data serves as the theoretical cornerstone for the protection of data rights and interests. Currently, there are

various viewpoints in academic circles, such as the theory of real right object, the theory of intellectual property right object, and the theory of intangible property right object. However, none of these can fully meet the needs of enterprise data protection. By distinguishing between primary data (e.g., user behavior records) and derivative data (e.g., results of user portrait analysis), the legal characteristics of different types of enterprise data can be revealed.

Secondly, it helps to reconstruct the rules for data interest distribution. The protection of enterprise data rights and interests involves multiple stakeholders, necessitating a balance among individual interests, enterprise interests, and public interests. By introducing the labor theory of value, it can be demonstrated that enterprises enjoy data property rights due to their resource investments in data collection, cleaning, and labeling. Meanwhile, based on the theory of data personality rights, enterprises are required to fulfill the "informed - consent" obligation to protect user privacy. This interest - balancing mechanism can not only incentivize enterprise innovation but also prevent data monopoly and abuse.

Thirdly, it innovates the data right allocation model. Traditional property rights theories are difficult to directly apply to enterprise data because of its non - exclusivity, non - rivalry, and other characteristics. By drawing on new - type right allocation models such as data trust and data usufructuary right, the separation of data control rights and usufructuary rights can be achieved.

2.2 Practical Significance

Firstly, it ensures the security of enterprise data assets. The protection of enterprise data rights and interests is directly related to their core competitiveness. By clarifying data ownership, enterprises can claim compensation for infringement damages in accordance with the law. For instance, in the case of Taobao suing Meijing Company, the court recognized for the first time that data possesses independent property - related rights and interests, setting a judicial benchmark for the protection of data assets.Secondly, it regulates the order of the data market transaction. The healthy development of the data trading market hinges on clear boundaries of rights and interests. By establishing a data ownership confirmation system, the standardization of data asset pricing can be promoted, and illegal transactions can be curbed. For example, the Shenzhen Data Exchange requires both trading parties to provide proof of data ownership, ensuring the legal origin of the data and facilitating the orderly circulation of data factors.Thirdly, it promotes the high - quality development of the digital economy. The protection of enterprise data rights and interests serves as an institutional guarantee for the development of the digital economy. By improving legislation, strengthening technological protection, and enhancing enterprises' governance capabilities, the cost of data leakage can be reduced, and enterprises' confidence in innovation can be bolstered.。

3 The Real - World Shackles Facing the Protection of Enterprise Data Rights and Interests in the Context of the Digital Economy

3.1 Imperfect Legal Regulatory Framework and Vague Boundaries of Rights and Interests

China's current legal system exhibits a fragmented approach to the protection of data rights and interests. Although the Civil Code includes data within its scope of protection, it lacks specific rules. The Data Security Law and the Personal Information Protection Law primarily focus on national security and privacy protection, leaving the definition and protection mechanisms for enterprise data property rights and interests inadequate. For instance, in the "Dianping v. Baidu" case, the court dismissed the plaintiff's claims on the grounds that the information posted by users did not constitute legal property rights, highlighting the legislative gaps that lead to difficulties for enterprises in safeguarding their rights.

Moreover, enterprise data often involves multiple stakeholders, including users, data collectors, and data processors. The law fails to clearly define the boundaries of rights and interests for each party. Taking the data of intelligent connected vehicles as an example, automobile manufacturers, vehicle owners, service providers, and public institutions all contribute to the data. However, the ownership of the data remains unclear, which is prone to triggering ownership disputes and increasing transaction costs.

3.2 Inconsistent Approaches to Judicial Protection and Chaotic Adjudication Standards

In judicial practice, the protection of enterprise data rights and interests is mainly achieved through avenues such as the Anti - Unfair Competition Law, the Copyright Law, and the Trade Secret Law. However, different courts exhibit discrepancies when applying these laws. For instance, in the "Sina Weibo v. Maimai" case, the court recognized user registration information as a property - related interest. In contrast, in the "Taobao v. Meijing Company" case, the court affirmed, for the first time, the independent property - related rights and interests of data. This inconsistency in adjudication standards makes it difficult for enterprises to predict the outcomes of their rights - safeguarding efforts.

In addition, some courts tend to regulate data infringement behaviors through the general clauses of the Anti - Unfair Competition Law. Nevertheless, these clauses lack specific provisions on "behavioral patterns and legal effects," making it challenging to provide clear adjudication guidelines. For example, in emerging infringement behaviors such as data scraping and traffic hijacking, courts often need to strike a balance of interests based on the facts of individual cases. This leads to a lack of predictability in the adjudication results.

3.3 Insufficient Technical Protection Capabilities and High Data Security Risks

As cyber - attack technologies advance, enterprise data is facing threats such as ransomware, DDoS attacks, and APT attacks. For example, an employee of a certain express delivery company leaked 400,000 pieces of customer information by renting out system accounts, resulting in an involved amount of over 1.2 million yuan. Such incidents reveal the technical weaknesses of enterprises in areas like data encryption, access control, and security auditing.In addition, to balance data circulation and privacy protection, enterprises need to anonymize data. However, existing technologies can hardly completely sever the link between data and individuals. As a result, anonymized data may still be re - identified. For instance, through multi - source data fusion analysis, attackers may reverse - engineer personal identity information, thus increasing the risk of data leakage.

3.4 Unsound Market Trading Mechanisms, Hindering Data Circulation

First, it's difficult to price and value data. Data, as an intangible asset, has its value influenced by factors like data quality, completeness, and timeliness. There's a lack of unified pricing standards. For example, in the data trading market, the price of the same data package can vary greatly depending on the different needs of buyers. This makes it hard for enterprises to realize the value of their data through market - based means.

Second, black - market trading is rampant. Data black markets obtain enterprise data through illegal means and then peddle it on the dark web and illegal trading platforms, seriously disrupting market order. For instance, user data from a certain e - commerce platform was sold at a low price on the black market, leading to customer loss and damage to the enterprise's brand reputation. Such actions not only harm enterprise interests but also destroy the fair - competition environment in the data market.

3.5 Lack of Interest - Balancing Mechanisms, Highlighting Multi - Party Conflicts

First, there is a conflict between enterprise data rights and interests and personal information protection. When enterprises collect and use user data, they need to balance data utilization and privacy protection. For example, enterprises achieve precision marketing through big data analysis. But if they don't fully inform users about how their data will be used or don't obtain valid consent, it may constitute an infringement of personal information. Such conflicts are particularly prominent in fields like finance, healthcare, and e - commerce.

Second, there is a contradiction between data monopoly and open sharing. To maintain a competitive edge, enterprises often tend to monopolize data resources and restrict data circulation and sharing. However, the nature of data as an element determines that it needs to be circulated to achieve maximum value. For instance, in the field of artificial intelligence, the phenomenon of data silos leads to insufficient training data for algorithm models, which restricts technological innovation. How to promote data open sharing while protecting enterprise data rights and interests has become an urgent issue to be solved.

4 Optimization Paths for the Protection of Enterprise Data Rights and Interests in the Context of

the Digital Economy

In the era of the digital economy, data has become a core element driving enterprise innovation and economic growth. The protection of its rights and interests not only concerns the survival and development of enterprises but also affects the overall ecosystem and competitiveness of the digital economy.However, at present, the protection of enterprise data rights and interests is facing multiple dilemmas, such as vague laws, backward technology, and a disordered market. It is urgent to explore optimization paths from dimensions like system construction, technology empowerment, market governance, and international coordination. This is to achieve a dynamic balance between the protection of data rights and interests and the release of data value.

4.1 Improve the Legal System and Lay a Solid Foundation for Rights and Interests Protection

First, promote specialized data legislation. Speed up the formulation of the Data Rights and Interests Protection Law or amend existing laws to clarify the legal nature, ownership definition, and protection rules of enterprise data. Draw on the experience of the EU's Data Act, distinguishing between types such as raw data, derived data, and trade secrets. Grant enterprises property - related rights and interests based on their data collection and processing investments, while also stipulating users' priorities (such as the right to know and the right to correction) based on their status as the original data sources.

Second, unify judicial adjudication standards. The Supreme People's Court can issue typical cases and judicial interpretations on the protection of enterprise data rights and interests to clarify the applicable boundaries of approaches such as the Anti - Unfair Competition Law, the Copyright Law, and the Trade Secret Law. At the same time, establish a rapid trial mechanism for data disputes to shorten the cycle for enterprises to safeguard their rights.

4.2 Enhance Technical Protection Capabilities and Build a Security Governance Barrier

Enterprises should adopt an integrated "end - pipe - cloud" protection system. At the data collection end, they can use privacy - computing technologies (such as federated learning and multi - party secure computation) to achieve "data availability without visibility." During the data transmission process, they should apply national cryptographic algorithms to encrypt sensitive data and combine them with blockchain technology to record and prove data circulation. In the data storage phase, they need to implement hierarchical and categorized data management. For core data, they should use hardware security modules (HSMs) for encryption and regularly conduct off - site disaster recovery backups. For example, financial enterprises process users' identity information in an isolated environment using trusted execution environment (TEE) technology to prevent data leakage.At the same time, enterprises should develop data - leakage tracing and emergency response technologies. They can use artificial intelligence and big - data analysis technologies to build an intelligent data - leakage monitoring system that tracks risk signals in real - time, such as abnormal access behaviors and data - forwarding records. They should also establish emergency response plans, clarifying the notification process, remedial measures, and responsibility - determination mechanisms after a data leakage occurs.

4.3 Regulate the Data Market Order and Promote the Orderly Circulation of Data Factors

First, establish a data property rights registration and trading system. Drawing on the model of intellectual property rights registration, the national data management department or third - party institutions should set up a data property rights registration platform. Enterprises can obtain data ownership certificates by submitting materials such as data source proofs and processing process descriptions. At the same time, efforts should be made to push data exchanges to improve their trading rules. They should formulate data quality assessment standards, pricing models, and contract templates to reduce transaction costs.

Second, severely crack down on data black markets and monopolistic behaviors. Departments such as public security and cyberspace administration should jointly launch special rectification campaigns. Using technical means like dark web monitoring and tracking of capital flows, they should combat illegal data collection and trafficking gangs. In addition, anti - monopoly law enforcement agencies need to pay attention to the data concentration trend of leading enterprises and prevent them from restricting competition through mergers, acquisitions, exclusive agreements, and other means.

4.4 Strengthen International Collaborative Governance to Address Challenges of Cross-border Data Flows

First, actively participate in the formulation of global data rules. We should vigorously promote the establishment of a multilateral data governance framework. In mechanisms such as the WTO negotiations on e-commerce and the DEPA (Digital Economy Partnership Agreement), we should advocate for the principle of "classified and tiered protection of data + secure cross-border data flow."

Second, establish a mechanism for resolving cross-border data disputes. We should encourage enterprises to sign agreements with their overseas partners that include "choice of dispute resolution clauses," specifying the application of Chinese law or the resolution of disputes through international arbitration institutions (such as the China International Economic and Trade Arbitration Commission).

5 Conclusion

In short, the protection of enterprise data rights and interests is a systematic project. It needs laws as the foundation, technology as the support, the market as the link, and international coordination as the guarantee. Through multi - dimensional optimization paths, we can not only effectively prevent risks such as data leakage and infringement but also unleash the value of data elements. This will drive the digital economy to develop in a higher - quality and more sustainable direction.

References

[1] Zhu, K. S. (2025). Research on the collection and management of corporate income tax for data assets. Taxation Research, (03), 99 - 104.
[2] Fu, D. P., Wang, H., & Guo, J. D. (2025). How does the market - oriented allocation of data elements enhance enterprises' new - quality productivity? — Based on the transmission mechanism of empowering the digital economic development of cities. Western Forum, 35(01), 22 - 35.
[3] Li, S. (2024). Research on the confirmation of enterprise data property rights in the digital economy era. Journal of Jiangxi University of Finance and Economics, (05), 110 - 122.
[4] Cai, W. Z. (2023). Legal protection and model construction of enterprise data in the digital economy era. Social Scientist, (12), 86 - 92.

Fund Project: Innovation Project of the Anhui Provincial Undergraduate Research Fund - "Research on the Protection of Enterprise Data Rights and Interests: From the Perspective of Intellectual Property Law"; Project Number: XSKY25048ZD
Author Bio: Zhiyao Jiang (2005 -), Han ethnicity, a native of Hefei City, Anhui Province, is an undergraduate student majoring in Foreign-related Rule of Law at the School of Law, Anhui University of Finance and Economics.