

The Difference And Synergy Between Data Rights And Data Interests

Chen Lu

China Jiliang University, Hangzhou, Zhejiang, 310018, China

ABSTRACT

In the era of digital economy, data has become a new type of production factor, making it crucial to clarify the connotations, attributes, and protection pathways of data rights and interests. Through conceptual analysis, this paper points out that data rights possess exclusivity, emphasizing control and dominance over data, while data interests exhibit diversity and openness, encompassing comprehensive benefits such as property and personality. Theoretically, the "bundle of rights" theory deconstructs the complex structure of data interests, with labor property rights and utilitarianism jointly driving the protection of data interests. Meanwhile, in the face of challenges such as difficulties in applying judicial adjudication rules and the fragmentation of legislative systems, a hierarchical rights confirmation system should be established, behavioral regulation mechanisms should be improved, and data governance should be achieved through multi-stakeholder co-governance. This paper aims to provide theoretical references for the improvement of China's data legal system and promote the healthy development of the data factor market.

KEYWORDS

Data rights; Data entitlements; Data governance

1 Introduction

The digital economy represents the trend of our times, with data increasingly gaining prominence as a new type of production factor. Legal regulatory issues surrounding data have thus become a focal point of research in the field of jurisprudence. Data interests and data rights are two key concepts in data legal systems. Clarifying their conceptual definitions, legal attributes, and practical protection pathways holds significant importance for establishing market rules for data factors and balancing the interests of data subjects with societal public interests. This paper conducts research from perspectives such as conceptual analysis, theoretical foundations, practical challenges, and institutional construction, aiming to provide academic support for the improvement of China's data legal framework.

2 Conceptual demarcation

2.1 Semantic boundary demarcation

2.1.1 The legal positioning of data rights

Data rights are legally granted control rights over data by data subjects, playing a pivotal role in regulating data circulation order and safeguarding the legitimate rights and interests of data subjects. For instance, personal biometric data such as fingerprints and facial recognition contain unique physiological information of individuals, who possess control over such data and have the right to decide whether it is collected, stored, or how it is used. Any organization or individual that collects or uses such biometric data without personal consent infringes upon the individual's data rights. From an enterprise perspective, commercial data collected during lawful business operations constitutes a vital asset for corporate operations and development, with enterprises enjoying property rights over such commercial data. Enterprises may analyze this data to uncover potential commercial value, formulate precise marketing strategies, while other enterprises are prohibited from unauthorized acquisition or use of such commercial data. These clearly defined data rights grant subjects autonomous control over data, establishing a rights-based foundation for data circulation and transactions in the market. Simultaneously, this enables data to become an economically valuable resource that circulates and is utilized within a lawful and orderly framework.

2.1.2 The multifaceted connotation of data rights and interests

Data rights refer to the comprehensive interests enjoyed by subjects through the generation, utilization, and circulation of data, encompassing a broad scope that reflects the complex interest relationships between data and subjects across various scenarios. In terms of property rights, platforms collect, organize, and analyze user data to develop diverse data products and services, generating economic benefits. The platform's right to profits derived from data value appreciation constitutes data property rights, as exemplified in the "Alibaba v. Meijing Case", where the court recognized that enterprises hold property rights over their data products. From the perspective of personality rights, users possess

the right to self-determination regarding their personal data. On social platforms, users have the authority to decide whether their posted content is public or visible to specific individuals, as well as the choice to accept or decline personalized advertisements based on their data. Furthermore, data rights also include more extensive interests. The public's right to access public data is a significant manifestation of data rights. Government agencies possess vast amounts of public data, which can facilitate scientific research, commercial activities, and improvements in daily convenience. The public has the right to demand that governments reasonably disclose such public data while ensuring data security, thereby maximizing the societal value of data. These multifaceted data rights, regulated and adjusted by laws governing data-related conduct, indirectly safeguard the legitimate interests of subjects in data activities.

2.2 The essential difference in legal attributes

2.2.1 The dichotomy between the rights model and the interests model

From the perspective of property rights ontology, there are significant differences between the data rights model and the data interests model in regulating data property relations. ^[1]The data rights model takes "rights confirmation" as its core tenet, aiming to establish exclusive rights similar to traditional property rights. ^[2]Under this model, enterprises possess ownership or quasi-property rights over the data they collect, organize, and process, granting them absolute control and the ability to exclude unauthorized interference or use by others. This facilitates long-term planning and in-depth development of data as core corporate assets, promotes specialized division of labor in data transactions, and enhances data utilization efficiency. However, in the context of data-sharing trends, such exclusivity may restrict data circulation, where overly stringent exclusive rights could hinder the free flow of data among different entities, thereby impeding the full realization of data value. In contrast, the data interests model is oriented toward "behavioral regulation," primarily protecting legitimate interests indirectly by prohibiting improper data utilization practices. A typical manifestation in practice is the regulation of data scraping under anti-unfair competition laws. When enterprises bypass authorization restrictions through improper means to scrape large volumes of data from others, such actions not only harm the legitimate interests of the scraped enterprises but also disrupt market competition order. Anti-unfair competition laws safeguard enterprises' lawful interests in data utilization by prohibiting such unfair scraping practices, thereby maintaining a fair competitive environment. This model does not require defining absolute ownership of data but instead emphasizes regulating data utilization behaviors, offering greater flexibility to adapt to the social nature of data and dynamic market conditions. Nevertheless, this model also suffers from insufficient protection intensity. In complex data disputes, the lack of clear rights delineation may make it difficult to accurately determine the rights and obligations of involved parties, increasing uncertainty in the protection of interests.

2.2.2 The tension between exclusivity and openness

Data rights possess strong exclusivity, which is a crucial characteristic for safeguarding subjects' control over data. When an individual requests a data processor to delete personal data, the processor is obligated to comply with legal provisions and the individual's request by performing the deletion operation, and must not retain or use such data without authorization. This reflects the individual's exclusive control over their data. The same applies to enterprises' proprietary rights to data usage—businesses enjoy exclusive rights to utilize data products and services, and other enterprises are prohibited from unauthorized use, which would otherwise constitute infringement. Such exclusivity helps protect the rights and interests of data subjects, preventing arbitrary violations and misuse of data. In contrast, data interests are more open in nature, emphasizing the balance of benefits among different entities in data utilization. Government agencies open public data to the general public and businesses to promote the realization of data's social value, drive technological innovation, economic growth, and enhance public services. In this process, it is essential to balance corporate commercial interests with societal public welfare. On one hand, businesses can leverage public data to develop innovative products and services, achieving commercial value; on the other hand, the openness of public data should ensure equitable access for the public to meet societal needs. This openness enables data to flow and be utilized more broadly, yet it also presents challenges in balancing the interests of all stakeholders. Legal frameworks must carefully consider the demands of different entities to maximize the benefits of data utilization while ensuring fairness.

3 The theoretical foundations of data rights and data interests

3.1 The "bundle of rights" theory of data interests

Professor Wang Liming's proposed "bundle of rights" theory has opened up a new paradigm for in-depth analysis of data rights and interests. ^[3] Over data, there often intricately interweave diverse rights claims from different subjects.

Among them, data generators such as individual users possess personal rights and interests that encompass multiple aspects, including but not limited to privacy protection of their own data, maintenance of data accuracy, and the right to informational self-determination. These personal rights and interests serve as the cornerstone for safeguarding individuals' basic dignity and rights in the digital world. Enterprises, as data processors, by virtue of their investment and labor in the processes of data collection, organization, analysis, and utilization, enjoy property rights and interests over data, granting them the right to leverage data for creating economic value and enhancing market competitiveness. At the same time, it is imperative not to overlook the public interest in data utilization, which manifests as the right to demand and reasonably use data for macro-level concerns such as public safety, public health, and social equity. These rights do not exist in isolation but are closely interwoven like a "bundle of rights," interrelated yet distinctly demarcated, collectively constructing the highly complex structure of data rights and interests. When users provide personal data to platforms, on one hand, they firmly retain the right to informational self-determination—a core manifestation of personal rights and interests—which determines critical issues such as whether personal data is used, how it is used, and within what scope. On the other hand, users also partially and conditionally relinquish the commercial use rights of data, enabling enterprises to utilize such data for business operations, thereby generating corporate property rights and interests. However, when platforms leverage such data for commercial activities, they must not act recklessly. They are obligated to strictly comply with public data security regulations, as this involves the broader societal public interest, pertaining to the stability, safety, and sustainable development of the entire society in the digital environment.

3.2 The dual drive of labor property rights theory and utilitarianism

3.2.1 The legitimacy of data rights from the perspective of labor property rights

Locke's labor theory lays a crucial theoretical foundation for the initial allocation of data rights.^[4] When processing entities extract value from data, they must undergo complex and time-consuming labor processes. First, during the data collection phase, processors acquire raw data from multiple sources, including online platforms and offline surveys. This raw data is typically disorganized and requires sorting before utilization. Second, data processing tasks such as cleaning and desensitization aim to eliminate erroneous, duplicate, and irrelevant data to make it usable. Thus, data cleaning personnel must employ specialized tools and algorithms to meticulously screen and filter the data to ensure its quality. Finally, professional algorithms and tools are employed for data analysis to uncover valuable information and patterns. Data analysts select appropriate algorithms and tools based on data characteristics and business needs to conduct in-depth mining and analysis. Through these labor-intensive stages, data processors endow raw data with economic value and are therefore entitled to property rights. When enterprises develop data products, they invest substantial human, material, and financial resources—assembling professional teams, establishing data collection systems, procuring hardware facilities, and covering salaries and R&D expenses. Consequently, enterprises' claim to property rights over data products aligns with the legal logic that "labor creates value," reflecting respect and recognition for the labor involved in data processing.

3.2.2 Utilitarianism's efficiency considerations in the protection of data rights and interests

From the perspective of maximizing overall social welfare, the protection of data rights should aim to achieve a balance between data utilization and innovation incentives. Overemphasizing the exclusive nature of data rights would severely hinder data circulation. Once data flow is obstructed, efficient interaction and collaboration among entities based on data become difficult, thereby stifling the innovative vitality essential for the thriving development of the digital economy and making its progress sluggish and slow. Conversely, completely neglecting the substantive protection of data rights may lead to rampant data abuse. Such abuse not only causes direct and severe harm to individual interests but also disrupts the social data ecosystem, ultimately imposing significant negative impacts on the collective welfare of society. The European Union's General Data Protection Regulation (GDPR), during its formulation and implementation, fully recognized the importance of personal data rights and reinforced them through a series of rigorous and detailed provisions. At the same time, it introduced the innovative institutional design of the "right to data portability" to facilitate data mobility. This right empowers data subjects to transfer their data from one data controller to another, enabling freer data flow within a lawful and compliant framework. This approach exemplifies the principle of pursuing a balance of interests under a utilitarian framework—safeguarding personal data rights while promoting the reasonable utilization of data to maximize overall social welfare.

4 Practical challenges of data rights and data interests

4.1 The dilemma of rule application in judicial adjudication

4.1.1 Conflict of dual attributes in personal data rights

Personal data possesses both personality rights and property rights attributes, giving rise to numerous conflicts of interest.^[5] In the context of online shopping, user data such as consumption records, browsing preferences, and purchasing behavior on e-commerce platforms contains personal privacy information. On one hand, users have the right to refuse excessive collection and use of such data by e-commerce platforms based on their privacy rights, safeguarding their personal information security and life tranquility. On the other hand, after integration and analysis, this consumption data can provide valuable market insights for e-commerce platforms, helping optimize product recommendations and formulate marketing strategies, thereby generating economic benefits. From a property rights perspective, as the generators of data, users expect to obtain corresponding economic returns by authorizing the use of their data. However, the current Personal Information Protection Law primarily focuses on protecting the personality rights attributes of personal data, emphasizing control rights, right to know, right to correction, right to deletion, etc., to prevent illegal collection, use, or leakage of personal information and protect personal dignity as well as the safety of life and property. Yet regulations on the property rights of personal data remain relatively lacking, with no clear rules on data control ownership or mechanisms for distributing data-derived profits. This leads to practical disputes over "data control ownership" and "data profit distribution" in scenarios involving data transactions and data sharing.

4.1.2 Divergent approaches to enterprise data protection

In judicial practice, corporate data protection approaches exhibit significant divergence, with landmark cases including "Alibaba v. Meijing" and "Tencent v. Zhejiang Soudao & Hangzhou Juketong Group Control Case". In the "Alibaba v. Meijing" case, Alibaba invested resources to develop a data analytics product that provided decision-making references. Meijing Company, without authorization, allowed others to use the product for profit, thereby infringing upon Alibaba's rights. The court ruled that operators of data products possess property rights over derivative data and should be protected accordingly. In the "Tencent v. Zhejiang Soudao & Hangzhou Juketong Group Control Case," the WeChat platform held vast amounts of user data, encompassing both personal privacy and aggregated data resources. The court, based on personal information protection rules, emphasized users' control over their data to safeguard personality rights. Simultaneously, the court recognized WeChat's competitive rights over integrated and analyzed data resources. This illustrates two distinct judicial approaches to data protection: "rights-based protection" and "conduct-regulation protection." "Rights-based protection" seeks to define specific types of corporate data rights, granting businesses exclusive, property-like control over data to ensure absolute authority and profit rights.^[6] Conversely, "conduct-regulation protection" primarily safeguards corporate data interests indirectly by prohibiting unfair competition practices. Each approach has its merits and drawbacks. "Rights-based protection" provides a clear legal foundation for data rights but may hinder data circulation and sharing. "Conduct-regulation protection" offers greater flexibility to adapt to diverse data utilization scenarios but suffers from weaker rights definition and enforcement, leading to inconsistent rulings in similar cases and undermining legal certainty and authority.

4.2 The issue of fragmentation in the legislative system

China's fragmented data legislation poses challenges to the protection of data rights and interests. Although the Civil Code recognizes data protection, it fails to specify concrete rights, resulting in a lack of operability. The Data Security Law focuses on data security but provides only principle-based provisions on enterprise and public data rights. The Personal Information Protection Law emphasizes personal information protection but inadequately regulates personal data property rights. The "Data Twenty Articles" propose a tripartite rights allocation framework, yet remain at the policy level without supporting legal mechanisms, making implementation difficult. This legislative landscape leads to blurred boundaries of data rights, insufficient coordination among laws, and hinders the development of data markets and value realization.

5 Institutional construction of data rights and data interests

5.1 Constructing a data rights system through hierarchical rights determination

5.1.1 Personal data: strengthening personality rights and limited property rights

Individuals possess the right to data self-determination, which constitutes the core of personal data rights. In the digital era, personal information such as life trajectories and consumption habits are recorded and stored, granting individuals the right to understand the collection, usage, and storage of such data. Software developers should clearly disclose the scope, purpose, and retention period of data collection, enabling individuals to make informed decisions regarding authorization. Individuals also retain the rights to access, correct, and delete their data. If erroneous information is identified, they may request platforms to make corrections; if they oppose the usage of their data, platforms should delete the relevant information. The increasing economic value of data underscores the necessity to recognize individuals' property interests in data commercialization. Data trusts serve as an effective mechanism to realize these rights—individuals entrust their data to fiduciary institutions, which manage and operationalize the data to maximize value while safeguarding privacy, subsequently distributing benefits back to individuals. Data brokers act as intermediaries, collecting and processing personal data before selling it to enterprises, from which individuals may derive compensation.

5.1.2 Enterprise data: establishing a "usage rights - profit rights" property rights framework

Enterprise data is categorized into raw data and derived data, requiring the establishment of distinct rights frameworks for each. Enterprises possess limited usage rights over raw data, meaning user consent must be obtained. Platforms are prohibited from using or selling raw data beyond authorized scopes to safeguard user data control and privacy rights. Derived data, however, grants enterprises exclusive property rights. Enterprises invest substantial human, material, and technological resources to collect, organize, clean, analyze, and process raw data, transforming it into derived data with higher commercial value. Since enterprises contribute creative labor to the formation of such derived data, they are entitled to corresponding property rights.^[7] Subsequently, enterprises can facilitate the market circulation of derived data through transactions, licensing, and other means, operating it as a critical corporate asset. The California Consumer Privacy Act (CCPA) establishes key regulations for enterprise data utilization, mandating that businesses provide consumers with transparent privacy policies and clearly disclose data processing practices to ensure consumer awareness and choice. Enterprises must obtain explicit consumer consent before selling personal data; otherwise, the sale of such information is prohibited. These provisions define the obligations and responsibilities of enterprises in data utilization, preventing misuse, protecting consumer rights, and ensuring lawful and orderly data circulation.

5.2 Improving the data rights protection mechanism with a behavior-oriented regulatory approach

5.2.1 Expanding the application of the anti-unfair competition law

In the field of data, behaviors such as data scraping and data misuse are commonplace, severely infringing upon the legitimate rights and interests of data controllers and disrupting market competition order. As a key legal instrument for maintaining fair market competition, the Anti-Unfair Competition Law should extend its application to the protection of data rights, regulating "non-credible data utilization practices."^[8] Unauthorized large-scale data scraping not only violates the data rights of the scraped platforms, depriving them of reasonable returns on their prior investments in human, material, and technical resources, but also undermines the fairness of market competition, thereby causing disorder in the market competition landscape. With the continuous development of the data economy, it is necessary to further clarify the exceptions to "data exclusivity." While safeguarding the legitimate rights and interests of data controllers, measures should be taken to prevent enterprises from abusing data rights to form market monopolies. When data involves special circumstances such as public interest or scientific research, reasonable use of data under specific conditions should be permitted to break data monopolies, promote data circulation and sharing, and drive social innovation and development.

5.2.2 Special protection of public data rights

Public data possesses social value and public attributes, thus establishing an open sharing system for public data is crucial. Governments and public institutions should clarify management responsibilities, formulate reasonable open plans and standards, and release data in unified formats and standardized interfaces to safeguard public access rights. Meanwhile, it is necessary to regulate the commercial utilization of public data to ensure social value is compensated. When developing intelligent mobility service applications, enterprises should pay fees to the government and comply with data security standards by implementing measures such as encryption and access control to prevent data leakage, tampering, or misuse, thereby ensuring data security and personal privacy. These measures can balance public interests

with corporate innovation, achieving reasonable utilization of public data and maximizing its social value.

5.3 Building a data governance system with the goal of pluralistic co-governance

5.3.1 The realization of rights empowered by technology

The decentralized, tamper-proof, and traceable characteristics of blockchain technology provide reliable support for data ownership registration. It can record the generation, storage, and circulation processes of data, ensuring clarity in data provenance and ownership. In data transactions, blockchain technology allows data owners to record ownership information and verify the legality and security of transactions through queries, thereby enhancing the certainty of data rights. Typical blockchain technologies include smart contracts and privacy-preserving computation techniques, both of which provide technical security for data utilization. Smart contracts are self-executing contracts based on blockchain, which establish data transaction rules in the form of code and automatically execute transactions that meet predefined conditions, avoiding human intervention and default risks while improving transaction efficiency and credibility. Privacy-preserving computation techniques include secure multi-party computation, federated learning, homomorphic encryption, and others, balancing data utilization with rights protection and ensuring secure data circulation and sharing.

5.3.2 Synergistic innovation in regulatory frameworks

Establishing a regulatory system of "legislative guidance-judicial adjudication-industry self-discipline" is an effective approach to data governance. Legislation should clarify the fundamental rules of data rights and interests, providing a legal basis for data activities. Judicial adjudication unifies standards through landmark cases, impartially resolving data infringement disputes, protecting the rights of data subjects, and reducing inconsistent rulings in similar cases. Industry associations should formulate self-regulatory conventions to standardize data activities, organize member enterprises to develop data classification and grading standards as well as transaction process specifications, promote the healthy development of the data industry, and form a collaborative governance framework.

6 Conclusion

The definition and protection of data interests and data rights essentially represent the legal reconstruction of rules governing the allocation and utilization of data elements in the digital era. While distinct from each other, they are closely interrelated—data rights serve as the core vehicle for data interests, providing an institutional foundation for data circulation through rights confirmation; data interests represent the extension of data rights, ensuring the social sharing of data value via multi-stakeholder interest balancing. Moving forward, it is imperative to construct a data legal system characterized by "clearly defined rights, comprehensive interest protection, efficient circulation mechanisms, and effective regulatory coordination" based on existing theoretical frameworks and China's current digital economic development. This will provide robust legal safeguards for the market-based allocation of data elements.

References

- [1] Du Muzhen. Similarities and differences between data rights model and equity model——Taking the ontological analysis of property rights as the approach[J]. *Journal of East China University of Political Science and Law*, 2024(4).
- [2] Yao Jia. The structure and dynamic comparison of data rights[J]. *China Applied Law*, 2023(3).
- [3] Wang Liming. On data rights: from the perspective of "right bundle"[J]. *Politics and Law*, 2022(7).
- [4] He Peiyu, Xu Jingran. The Legal Dilemmas and Solutions for Data Rights Protection in China [J]. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)*, 2024(5).
- [5] Li Xiaoyu. Typical Protection of Data Rights and Interests from the Perspective of Distinguishing Rights and Interests [J]. *Intellectual Property*, 2019(3).
- [6] Ding Xiaodong. On the Legal Protection of Enterprise Data Rights and Interests: An Analysis Based on the Legal Nature of Data [J]. *Science of Law (Journal of Northwest University of Political Science and Law)*, 2020(2).
- [7] Sun Ying. On the Basic Categories of Data Rights Object [J]. *Oriental Law*, 2024 (1).
- [8] Mei Xiaying The Original Theory of Enterprise Data Rights: From Property to Control [J]. *Chinese and Foreign Law*, 2021(5).