WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 1
HASS 2023

Analysis of the Path of Protecting Enterprise Data Rights and Interests in China

Ruwei Liu *

School of Law, Wuhan University, Wuhan, China

* Corresponding Author Email: 1203746762@qq.com

Abstract. In the era of big data, data has gradually become the most important production factor and resource for enterprises, and disputes caused by enterprise data have also emerged endlessly. The existing framework for protecting enterprise data rights and interests in China has many shortcomings in theory and practice, which cannot properly solve problems and is not conducive to the development of the digital economy. Therefore, it is urgent to establish a protection method for enterprise data rights and interests. Due to the unique nature of enterprise data and its complex relationship with personal data, the protection of enterprise data rights cannot be generalized. According to the main forms of enterprise data disputes and the current situation of the main sources of enterprise data in China, it is appropriate to design corresponding rights from the perspectives of "enterprise-enterprise" and "enterprise-individual" to protect the rights and interests of enterprise data. Based on the establishment of restrictive property rights for enterprise data, when adjusting the rights and attributes of personal data, we aim to construct a path for protecting the rights and interests of Chinese enterprise data and promote the prosperity and development of the market economy and digital economy.

Keywords: Enterprise Data; Personal Data; Property Right.

1. Introduction

With the rapid development of information technology, the connection between data and human society has become unprecedentedly close, and data has become the most critical component of enterprises. Enterprise management, analysis, and collection of a large amount of data have formed valuable and sensitive enterprise data, gradually becoming the most important production factor and competitive advantage of enterprises. It is precisely due to the importance of enterprise data that the number and forms of disputes have increased in recent years. However, China has not yet implemented specific laws and regulations to transfer data rights to enterprises. This leads to attempts to seek solutions from existing laws when adjudicating and resolving various cases related to enterprise data disputes. However, the existing legal system developed based on traditional tangible goods is at a loss when faced with the unique characteristics of enterprise data in terms of form, usage, and other aspects. This discomfort undoubtedly hinders the resolution of disputes and the promotion of social and economic development. Therefore, it is urgent and fully necessary to establish a reasonable path for protecting the rights and interests of enterprise data, in order to identify and stop disputes and promote the development of the digital economy.

2. The Existing Legal Framework for Protecting Data Rights and Interests of Chinese Enterprises

The enterprise data protection framework in China integrates the protection of personal and corporate data. Because most enterprise data are based on personal data, the exercise of data rights by enterprises needs to take into account the requirements of personal information protection, that is, whether it is the retention, utilization, or transfer of enterprise data, the basic premise should be the legitimate processing of personal information.

2.1. The Protection of Enterprise Data at the Public Law Level

Article 285 (2) of the Criminal Law, stipulates the crime of illegally obtaining computer information system data. Since the establishment of the crime, most of it has been used by enterprises and individuals to illegally steal and use the data of companies and individuals through certain means. [1] In addition, Article 219 of the Criminal Law also stipulates the crime of infringing on trade secrets. In addition to the definition of trade secrets, the protection of trade secrets of enterprise data must also meet the result element of "causing great losses to the obligee".

2.2. The Protection of Enterprise Data Rights and Interests at the Private Law Level

2.2.1. Anti-unfair Competition Law

The Anti-unfair Competition Legislation is formulated in the context of adapting to the objective requirements of establishing and developing a socialist market economy and increasingly extensive international economic and trade cooperation and exchange and protecting the legitimate rights and interests of operators and consumers. Meanwhile, it also shoulders the responsibility of protecting consumer rights, maintaining a benign market competition order, and promoting healthy economic development. Although Anti-unfair Competition Law does not belong to simple private law, it has the nature of integrating public and private law. However, as a legal norm for adjusting property relations between equal subjects, the private law attribute of the Anti-unfair Competition Law is more profound. [2] In enterprise data disputes, the Anti-unfair Competition Law mainly addresses issues of infringement nature. Therefore, the author believes that the Anti-unfair Competition Law belongs to the category of private law.

(1) Adherence to business ethics

In most data dispute cases involving Internet companies, courts ultimately rely on Article 2 of the Anti-unfair Competition Law as the specific legal basis, which states that companies must not violate business ethics. In this case, the court generally believes that the crawler protocol is a widely recognized and accepted standard of conduct in the internet field, with recognized and general characteristics, and belongs to recognized business ethics. The violation of the basic norms of this industry belongs to the violation of the business ethics of the Internet industry, and therefore the general provisions of the Anti-unfair Competition Law apply.

For example, in cases such as the illegal seizure and use of user information on Sina Weibo by Maimai, the dispute over Baidu v. Qihoo 360 violating the "Robots Agreement" in crawling data, and the dispute over unfair competition between Dianping.com and Aibang.com [3], the court's recognition of the nature and legal status of the crawler agreement is not entirely the same, but they all agree that Internet companies should comply with the crawler agreement, and thus recognize "complying with the crawler agreement" as business ethics, Thus applying the Anti-unfair Competition Law.

(2) The protection of business secrets

If the relevant information contained in enterprise data has already constituted trade secrets, the protection of trade secrets will also cover the rights and interests of enterprise data. For data information with commercial values, enterprises may protect it through corresponding confidentiality measures. Therefore, the protection system of trade secrets can greatly protect the data rights and interests of relevant enterprises.

In addition, in order to obtain the protection of trade secrets, different legal provisions must be met. For example, in the field of intellectual property and anti-unfair competition, enterprise data must meet the requirements of non-disclosure, commercial value, and confidentiality measures. In labor law and company law, the protection of business secrets for enterprise data is limited to specific entities, or based on the existence of contractual relationships, and business secret protection is not targeted at unspecified third parties.

2.2.2. Civil Code

Disputes related to enterprise data can be remedied through the application of contract law and tort law, given that there is a pre-existing contractual arrangement between the two parties. However, no matter how meticulous this contractual arrangement is, it is only a form of debt protection and does not have exclusivity. It cannot be used to deal with data harm from third parties, and in reality, data harm often refers to the intrusion or illegal use of third parties outside the contractual relationship of enterprise data. [4]

2.2.3. Intellectual Property Law

If the information content contained in enterprise data has already constituted the object of intellectual property protection, such as software or e-books, then the copyright protection of works obviously indirectly protects the rights and interests of enterprise data. However, a large number of industrial and commercial data rarely directly constitute original works that meet the requirements of intellectual property rights. [5] Instead, it becomes enterprise data with rich commercial value through the convergence, sorting, and processing of enterprises.

3. The Shortcomings of the Protection of Corporate Data Rights in China

3.1. The Theoretical Level

Firstly, the existing legal framework is limited by the traditional private law rights thinking model, avoiding the confirmation of corporate data rights or adopting guiding clauses instead of clear provisions. [6] It is better to search for terminology to express the interests of enterprise data between existing property rights, claims, and intellectual property rights. The result is often difficult to justify in legal terms, especially the inability to handle the tense relationship between data sharing and exclusivity, disclosure and control, and technology carriers and information content. Each theoretical solution has limited coverage and many exceptions. [7]

Secondly, for the protection of data rights and interests of enterprises, the application of competition law provisions has always been a “temporary measure” rather than a “master key” to solving problems. The use of competition law clauses or licenses to solve problems in individual cases cannot be used to protect the rights and interests of enterprise data in all situations. The application of this general clause largely depends on the judge’s understanding of the clause. Due to the unpredictability and lag of written law, although judges are allowed to interpret the law in certain situations, excessive reliance on the judge’s inner balance of advantages and disadvantages can bring great uncertainty, which is not conducive to the stability of the law and the normative expectations of the parties.

3.2. The Practical Level

Firstly, the relevant provisions on personal information protection in the Personal Information Protection Law stipulate that personal information processing usually requires the consent of the information subject, which seems self-evident. However, in practice, network information service providers often fulfill their disclosure obligations through documents such as privacy policies and personal information protection policies and give individuals the opportunity to click on their consent. Compared to offline notification, notification in cyberspace is hardly equivalent to being informed by the defendant. The implementation of the consent rule faces difficulties, and may even become non-existent, resulting in the failure of the personal information protection system based on this framework. [8] At the same time, the unique nature of networks and data makes it difficult for contracts, infringements, and intellectual property rights in the Civil Code to be widely applicable, and their applicability is extremely limited.

Secondly, although as the law with the highest frequency and most widespread application in resolving data disputes between enterprises in practice, whether it is the application of anti-unfair competition law or trade secret related clauses, there are always significant limitations on the scope

and degree of enterprise data protection. In reality, enterprise data disputes continue to arise, even with the potential to erupt, involving the copying, theft, intrusion, and even competition of enterprise data, some of which occur between large companies. For example, SF Express announced the shutdown of Cainiao Data, sparking a dispute over data control rights. There is a viewpoint that both SF Express and Cainiao claimed in their statements that they attach the greatest importance to user data and are protecting it, but in reality, they are competing to control the data security protection market, and their valuation volume may have reached hundreds of billions of yuan. [9] These disputes have not been properly resolved under the adjustment of competition law, and often end up being intervened by the state or simply left unresolved.

4. The Attempt to Protect the Rights and Interests of Enterprise Data from the Perspective of Comparative Law

Enterprise data originates from the development and application of information technology and the development of the digital economy. The protection of enterprise data rights and interests is not limited to the protection of enterprises but also includes the protection of personal data. This study selects the processing methods for corporate and personal data-related issues in the United States and the European Union, which have developed information technology earlier and the digital economy more developed today, in order to provide useful ideas for protecting the data rights and interests of Chinese enterprises.

4.1. America

4.1.1. CLOUD Act and Enterprise Data

On March 23rd, 2018, the United States passed the Clarify Lawful Overseas Use of Data Act (CLOUD Act) to address disputes over how and when the United States and other countries can access data stored on third-party data platforms' cloud servers within each other's legal jurisdictions and to address cross-border data platform retrieval disputes. The bill clarifies that US law enforcement agencies have the power to obtain electronic communication data across borders, which means giving US courts nearly unlimited jurisdiction [10] to allow companies to keep their data overseas and submit it. This behavior is likely to lead to the company violating the laws of other countries or causing concerns among enterprise users about the leakage of data stored on the platform provided by the company, thereby affecting the operation and management of the enterprise.

4.1.2. The US Method for Enterprises to Restrict Data Capture Behavior Disputes

In the face of disputes over data capture restrictions, US courts mainly apply the theory of interference infringement to resolve them. Interference torts are considered an independent type of infringement, and the theory of interference torts holds that anyone who interferes with the economic relationship between others and third parties without justifiable reasons should be liable for compensation, including both contractual and expected contractual relationship [11]. Correspondingly, in disputes over restricted data crawling, companies that have been restricted from data crawling can demand compensation from companies that have made restrictions on data crawling on the grounds that the act of restricting data crawling has damaged their economic relationship with third parties. For example, in the hiQ v. LinkedIn case in the United States, hiQ Company accused LinkedIn of violating existing contracts and expected economic relationships by restricting data crawling, thus filing a claim for infringement of interference. However, this theory requires the existence of a contract between the two parties, which also has limitations and cannot be applied when there is no contract or an expected contract. It may also harm legitimate restrictions on data crawling, hindering another enterprise from protecting its legitimate interests.

4.1.3. Personal Information Data Legislation

On January 1st, 2020, the California Consumer Privacy Act (CCPA) was officially implemented. Subsequently, Illinois, New York, and Washington were all contemplating their own personal

information protection laws. The continuous emergence of local legislation has also promoted unified legislation at the federal level. On November 26th, multiple Democratic senators jointly proposed the Consumer Online Privacy Act (COPRA). [12]

However, the separate legislative model in the United States fully implements the principle of "Autonomy of Will" and may even be overcorrected, with data protection largely relying solely on market regulation and industry autonomy, which is beneficial for the circulation and utilization of information. However, due to the lack of unified legal rules to protect personal information, the collection, utilization, and processing of personal information are completely entrusted to the enterprise and resolved through contractual relationships with the rights holders of personal information, which may result in unfavorable protection of personal information. Especially in situations where financial resources, social status, and information acquisition capabilities are highly unequal between individuals and enterprises, it can ultimately legitimize the improper collection, use, and transfer of personal information by enterprises, making it difficult for individuals' rights to be fully protected [13], resulting in unfair competition between enterprises, ultimately leading to market imbalances and hindering economic development.

4.2. GDPR in the European Union and the Protection of Enterprise Data Rights and Interests

The violation of human rights by German fascism during World War II led to the EU being more comprehensive and advanced in protecting individual rights. In the field of data, this protection is specifically reflected in the General Data Protection Regulation (GDPR) of the European Union. The predecessor of this regulation was the Data Protection Directive formulated in 1995, which was revised and fully implemented in 2018. [14]

The Regulations give personal data subjects more comprehensive and specific rights compared to China, and the protection and supervision of personal information have reached an unprecedented level. They also impose stricter restrictions on the processing of personal data on data controllers. For instance, the principle of informed consent for the use of personal data is also more specific and stricter compared to the broader and more general legal language in China. The EU's standards clearly stipulate that users are required to "freely consent with full knowledge". [15] GDPR's unprecedented protection of personal data means expanding the obligations of enterprises as data controllers and processors, Specifically, in order to meet the high compliance requirements of GDPR, enterprises need to invest a large amount of manpower and financial resources to fulfill more obligations and responsibilities, which also means huge unified law enforcement costs. [16] This raises increasing doubts about whether the regulations can achieve the goal of enhancing the competitiveness of the European Union's digital economy. That is to say, the ultimate goal of GDPR is to promote the free flow of personal information within the EU while also promoting the development of the digital economy [17]. The means to achieve this goal is to strengthen citizens' personal information protection rights, but the actual results may backfire and deviate from its original intention.

Therefore, shortly after GDPR came into effect, the European Commission began to formulate a system to promote data circulation, utilization, or sharing, in order to alleviate or correct the shortcomings of GDPR. On November 25th, 2020, the European Commission proposed a Proposal for Data Governance Regulations to the EU legislative body, aimed at promoting data sharing among various departments and member states and making data sharing a key pillar of data strategy. In 2022, the Data Law Proposal was proposed to ensure legal data sharing and use between enterprises, in order to create a fair data economy. The two proposals share a common goal and content, both of which aim to solve the problems brought about by GDPR by granting enterprises more permissions and rights to data, in order to better promote the development of the digital economy.

5. The Design of Rights for Data Rights Protection of Chinese Enterprises

Based on the current framework for protecting corporate data rights in China and the corresponding processing methods of the European Union and the United States, this paper designs the rights of property rights and personal data rights from the perspectives of enterprise and enterprise, as well as enterprise and individual, based on the property rights of corporate data rights. We hope to form a more suitable method for protecting corporate data rights.

5.1. "Enterprise-enterprise": The Right Design of Enterprise Data Rights Protection Between Enterprises

Nowadays, data has been considered a core element of the new economy and has become one of the most commercially valuable elements. [18] As the most important data collection, processing, and user, legal disputes related to data between enterprises have emerged. With the development of data processing technology and the improvement of social and data integration, it is the general trend that the number of legal issues about data rights between enterprises increases and becomes more complicated. Simultaneously, due to the unique characteristics of data itself, the existing traditional legal framework based on the development of the industrial era is no longer able to properly resolve disputes related to data rights between enterprises. These data disputes will not only cause damage and frustration to data companies but also cause tremendous turbulence to the data market and social order in China. In response to disputes between enterprises caused by enterprise data, corresponding rights design needs to be carried out in this path to play a role in resolving disputes and promoting the development of the digital economy.

5.1.1. Defining the Nature of Enterprise Data Rights and Interests

Enterprise data and data cannot be completely equated. Enterprise data is the data collected, analyzed, and processed by enterprises through their designed methods or created platforms, and has certain commercial value. Simple data cannot become the protected object of this property right. As mentioned before, other paths that rely on existing rights systems for enterprise data protection, such as intellectual property paths, competition law paths, and other traditional private law paths, have their own practical and theoretical shortcomings, as well as application limitations. It fully demonstrates that the existing right path cannot solve the problem of protecting enterprise data rights and interests, and must rely on the newly established right path. Based on the following two reasons, it is appropriate to define enterprise data rights as property rights.

(1) Starting from the development law of the data economy

According to labor principles [19], the incentive effect of property rights [20], and the Coase theorem [21], enterprises invest a large amount of capital and human resources driven by data interests, and data becomes enterprise data due to the labor factors invested by the enterprise. The willingness and efforts of enterprises to support data development ultimately depend on whether their data can receive sufficient, reasonable, and effective legal protection. The biggest source of data benefits is market transactions, and clarity of property rights can improve market transaction efficiency and optimize efficiency. The existence of enterprise data property rights provides the most basic driving force and guarantee for the investment and reasonable conduct of enterprise data activities, and also clears unnecessary obstacles for transactions in the market, ultimately achieving the optimization of resource allocation.

(2) Starting from the existing legal provisions

Article 127 of the Civil Code, which is reserved from Article 127 of the General Rules of Civil Law, directly highlights the concept of "virtual property on the Internet". It is an abstract summary of certain resources on the Internet, clarifying the property attributes of such resources, and is the first step in property rights protection of virtual property. Although the legal provisions only specify online virtual property, it is not difficult to find commonalities between enterprise data and online virtual property based on their nature. Network virtual property is an information resource that exists in a

digital form in the network environment, which is relatively independent, has a certain degree of exclusivity, and has value and usefulness. Possessing and using virtual property on the Internet will bring wealth to the rights holders. Infringement of others' virtual property on the Internet can result in loss of property interests for the rights holder. [22] As one of the most commercially valuable production factors in enterprises, enterprise data has similarities with network virtual property in terms of its form, value, usefulness, and the consequences of others infringing on the rights and interests of enterprise data. Combining the principle of analogical application in legal thinking, adopting a path of property rights protection for enterprise data should be a reasonable and natural approach.

However, at present, this provision belongs to a general and declarative legislative model, and it cannot be used as a direct basis when resolving specific disputes. The specific legal basis for how to identify the nature of enterprise data and how to protect it by law remains to be resolved through separate laws.

5.1.2. Setting Restrictions on Enterprise Data Rights and Interests

The unique nature of enterprise data itself necessitates limitations on the property rights granted to enterprise data. Enterprise data itself has the complexity of data sources and the interweaving of interests involved. This leads to the design of the path for protecting enterprise data property rights, although in the form of private rights, which is different from typical property rights in civil law. It needs to take into account the protection requirements of multiple functions and interests [23], specifically presented as restrictive property rights design. The specific content of restricting property rights is based on the purpose of setting up property rights. The main purpose of setting restrictions on property rights for enterprises is to promote the development of the digital economy, protect personal information rights, and avoid disorderly competition among enterprises. Therefore, the design of restrictions should also reflect the above objectives.

Restricted property rights mean that enterprises do not enjoy the absolute exclusive property rights of traditional civil law to corporate data, but should be given the ability to resist improper acquisition of benefits from corporate data by others. When facing other enterprises, enterprises have exclusive rights to possess, use, and benefit from enterprise data. The law should be able to impose sanctions on entities that illegally leak, steal, or utilize enterprise data. Only in this way can enterprises create and process data in a stable and secure market environment, bringing greater social benefits. In addition, in order to protect this right, the urgent issue to be resolved in practice is the definition of enterprise data, especially whether the public data on the enterprise creation platform belongs to enterprise data. This study argues that, in addition to the common "sweat on the forehead" criterion, for publicly available data on the platform, although this portion of data is directly left by users on the platform and the enterprise may not seem to have paid "sweat on the forehead", in reality, the enterprise has invested a certain amount of energy and resources to create and operate the platform. Therefore, this portion of data should also belong to enterprise data, rather than something that other enterprises can freely access. That is, the enterprise also has property rights to this part of the data.

Because enterprise data is not generated out of thin air, for the vast majority of enterprises, the basic source of their enterprise data is users' personal data. Enterprises use mining, integration, and other creative means to turn users' personal data into enterprise data. Without personal data, there is no corporate data. Users share their data with the enterprises, so corporate data rights inevitably include some personal data rights. Therefore, when sharing, utilizing, or disposing of enterprise data, enterprises should follow a series of guidelines and restrictions, and make certain restrictions on the disposal rights related to the possession, use, and income of enterprise data, in order to avoid the property rights that enterprises have over enterprise data from causing harm to other interests. [24]

5.2. "Enterprise-individual": Driving Enterprise Data Rights Protection with Personal Data Rights Protection

Personal data and corporate data are closely connected. As the "raw material" of most corporate data, the relevant regulations on personal data rights will inevitably affect the exercise of corporate data rights. In this case, adjusting the attributes of personal data rights and interests indirectly improves the protection of enterprise data rights and interests by shifting the recognition of personal data rights and interests from emphasizing personality rights to appropriately incorporating property rights attributes.

5.2.1. The Correlation Effect of Personal Data Rights Protection on Enterprise Data Rights Protection

Constrained by the inertia of data ownership that should be traced back to the source entity [25], the gap in economic strength and social status between individuals and enterprises, combined with the purpose of protecting privacy and sensitive information, as well as the principle of legal protection of the weak, from the perspective of completeness of relevant regulations and judicial practice, China and the European Union are similar in terms of protecting personal data far more than protecting enterprise data.

Meanwhile, the legislation in China does not clearly distinguish between personal data and personal information. In addition, due to the development of science and technology, it is becoming increasingly difficult to distinguish between "personal data" and "personal information" in practice, resulting in a high degree of overlap between the rights attributes of personal data and personal information. From the current perspective, the definition of personal information [26] means that personal information involves more personality elements. Therefore, as long as the right to personal information is recognized as a civil right, then the right to personal information should be considered as a personality right [27]. Correspondingly, the definition of the right attributes of personal data naturally leans towards personality rights, while almost ignoring the property rights attributes of personal data. However, overemphasizing the attributes of personality rights while neglecting the attributes of property rights often leads to an imbalanced definition of rights in practice, which goes against the original intention of legislation and ultimately inevitably affects the data rights and interests of enterprises.

If the personality rights attribute of personal data is overly strengthened rather than the property rights attribute [28], once the personal ownership of the data is considered an inalienable personality right, then the collectors and users of the data cannot restrict the free exercise of such data rights. Just as private individuals cannot restrict citizens' free use of personal names through contracts, enterprises cannot demand individuals to relinquish their data rights through contracts [29]. This means that as long as any institution obtains this data through technological means, enterprises cannot hold it accountable, which is equivalent to losing property rights to user data on the platform they create. This will inevitably undermine the enthusiasm of enterprises, institutions, and innovative data platforms that have invested huge resources in utilizing data to recreate and reprocess user data. The digital economy has demonstrated that the processing and creation of data by enterprises is far more socially meaningful and economically beneficial than a simple collection of personal data. Overstrengthening the personal rights and interests of data suppresses the enthusiasm of enterprises and is not beneficial for the development of the social economy.

5.2.2. Improving the Protection of Enterprise Data Rights and Interests Through Reasonable Protection of Personal Data Rights and Interests

Personal information protection is not an obstacle to enterprise data protection, nor is the protection of enterprise data a limitation on personal information protection. On the contrary, the processing of data by enterprises is an important way to unleash the value of personal information. [30] Reasonable protection of personal data rights and interests is an important method to make enterprise data rights and interests protection more reasonable and effective.

(1) Reasonable restrictions on the rights and interests of enterprise data by preserving the personality right attribute of personal data

Against the backdrop of the constant suspension of the "Sword of Damocles" in personal information protection, fully protecting personal information is the bottom line and ultimate value, which cannot be changed. When adjusting the rights attributes of personal data, the retention of personality rights attributes cannot be ignored. At the same time, emphasizing the property rights attributes of personal data is beneficial for promoting enterprises' enthusiasm for data recreation, while retaining the personality rights attributes can impose certain restrictions on the property rights of enterprise data rights.

The personality right attribute of personal data should be to protect the interests of natural persons in the process of their personal data being collected, stored, transferred, and used by others, [31] and to prevent enterprises from arbitrarily using this data. When building a right barrier for natural persons to prevent illegal collection, use, and transfer of personal data by enterprises, thereby endangering their personal dignity and freedom, it indirectly restricts the property rights of enterprise data. Given the inequality between individuals and enterprises in social status, economic strength, information acquisition ability, and other aspects, the law should pay special attention to providing individuals with certain protection and convenience in terms of evidentiary responsibility, the statute of limitations, etc., in order to achieve substantive fairness and better protect the personality rights attributes in personal data rights.

(2) The property rights attribute of personal data rights promoting enterprises to utilize data resources

Personal information is crucial for the healthy operation of the entire business environment. The market economy is a credit economy, and all connections in the process of social reproduction are based on credit. Credit has become a key element in maintaining market order and economic development. In the context of the credit economy, establishing a sound and perfect social credit system is related to the economic operation of the entire society. [32] Only when personal information can be appropriately protected can it cultivate consumer trust, and individuals as consumers can confidently provide their personal information, allowing for the utilization of personal information throughout the entire business field. The property rights attribute of personal data rights, from the perspective of protecting property rights, has the attributes of encouraging transactions and maintaining market economic order that civil law has, because it can better maintain the credit relationship between both parties, thereby promoting enterprises to use personal data rights more efficiently and stably.

References

[1] By November 27th, 2022, there were 1,651 documents searching for "the crime of illegally obtaining data from computer information system" in criminal cases of China Judgment Document Network.

[2] Xue Jun. The connotation and application mode of platform responsibility in E-commerce Law [J]. Legal Science (Northwest University of Politics and Law Journal), 2023, 41(01): 57-68.

[3] Zhang Ping. General provisions of the Anti-Unfair Competition Law and its application-reflections on the search engine crawler agreement [J]. Application of law, 2013(03): 46-51.

[4] Long Weiqiu: Re-discussion on the path of property rights of enterprise data protection [N]. People's Court, 2018-11-08(005).

[5] Ji Hailong. Positioning and protection of data in private law [J]. Law Research, 2018, 40(06): 72-91.

[6] Article 127 of the Civil Code: "If the law has provisions on the protection of data and network virtual property, such provisions shall prevail".

[7] Mei Xiaying. On the rights and interests of enterprise data: from property to control [J]. Chinese and foreign law, 2021, 33(05): 1188-1207.

[8] Lv, Bingbin. Personal information protection "consent" dilemma and its way out [J]. Legal and business research, 2021.

[9] Behind the SF and Cainiao dispute: another billion-dollar market is hidden outside the data, contained in China Business Network http://www.ccwin.cn/article- 56540-1.html, March 25, 2018; CnBeta: Ma Yun and SF broke up

yesterday, and today they are reconciled. What is the data dispute? https://www. cnbeta.com/ articles/tech/ 618383. htm, March 25, 2018.

[10] CLOUD Act stipulates that "regardless of whether communications, records or other information are stored in the United States, service providers shall keep, back up and disclose communications, records or other information in accordance with the obligations stipulated in this chapter, as long as the above communications, records or other information are owned, monitored or controlled by the service provider".

[11] Gao Jiancheng. Identification of the illegality of restricting data capture from the perspective of American interference infringement theory [J]. Financial Law, 2022(06): 81-95.

[12] Xuke: Review of Top Ten Events of Global Data Governance in 2019. https://www.esensoft.com/industry-news/dx-5221.html

[13] Wang Liming. The legal protection of personal information rights-centering on the boundary between personal information rights and privacy rights [J]. Modern Law, 2013, 35(04): 62-72.

[14] Directive 95/46/ EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[15] Article 7 of GDPR: Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

[16] According to the survey data of Pricewaterhouse Coopers, 68% of American companies expect to spend $1 million to $10 million to meet the compliance requirements of GDPR; Another 9% of enterprises are expected to spend more than $10 million.

[17] Gao Fuping. The institutional defects of GDPR and its warning to the implementation of China's Personal Information Protection Law [J]. Research on the Rule of Law, 2022(03): 17-30.

[18] Zhao Lei. The legal significance of data property type [J]. Journal of China University of Political Science and Law, 2021(03): 72-82.

[19] Locke: On government (below) [M], Beijing Commercial Press, 1964. Locke believes that when people exert labor on something, the labor produces property rights.

[20] Xavier: Basic Theory of Legal and Economic Analysis, Renmin University of China Press, 2013. Xavier believes that property rights provide incentives for work and improve work enthusiasm and social benefits.

[21] As long as the property right is clear and the transaction cost is zero or small, then no matter who the property right is given at the beginning, the final result of market equilibrium is efficient and Pareto optimality of resource allocation can be achieved.

[22] Yang Lixin. The meaning and important value of network virtual property stipulated in the general principles of civil law [J]. Oriental Law, 2017(03): 64-72.

[23] Long Weiqiu. Re-discussion on the property right path of enterprise data protection [J]. Oriental Law, 2018(03): 50-63.

[24] Ji Leilei. Judicial Dilemma and Breaking Dimension of Enterprise Data Protection: The Road to Typing Right [J]. Law Forum, 2022, 37(03): 109-121.

[25] Yao Jia. Guidelines for the use of enterprise data [J]. Tsinghua Law, 2019,13(03): 114-125.

[26] Personal information refers to an identifiable symbol system associated with a specific individual and reflecting individual characteristics, including personal identity, work, family, property, health and other aspects of information.

[27] Wang Liming. On the legal protection of personal information rights-centering on the boundary between personal information rights and privacy rights [J]. Modern Law, 2013, 35(04): 62-72.

[28] Ding Xiaodong. What is data right? -Looking at the protection of data privacy from the European General Data Protection Regulations [J]. Journal of East China University of Political Science and Law, 2018, 21(04): 39-53.

[29] Ding Xiaodong. Who does the data belong to? -Looking at the ownership and protection of platform data from the perspective of Web crawler [J]. Journal of East China University of Political Science and Law, 2019, 22(05): 69-83.

[30] Wang Yegang. Outline of the relationship between enterprise data rights and personal information protection [J]. Comparative Law Research, 2022(04): 33-44.

[31] Cheng Xiao. On personal data rights in the era of big data [J]. China Social Sciences, 2018(03): 102-122+207-208.

[32] Zhang Xinbao. From Privacy to Personal Information: Theory and Institutional Arrangement of Interest Re-measurement [J]. China Law, 2015(03): 38-59.