Science of Law Journal (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2025.040411
ISSN 2616-2296 Vol. 4 Num. 4

Competition Law Path Advantage for Enterprise Data Protection

Tianlu Jia[1,*]

[1]School of Law, Guilin University of Electronic Technology, Guilin, 541000, Guangxi Zhuang Autonomous Region, China
**Corresponding author*

Keywords: Enterprise data; anti-unfair competition law; enterprise dataprotection; unfair competition behavior

Abstract: Against the background of the ever-expanding value of data, the protection of data has also attracted constant attention, and the path of protection of enterprise data and the rules of adjudication of such behavior in judicial practice have not fully formed a universal paradigm. In this case, what kind of ways should be adopted to regulate the improper acquisition and use of enterprise data, and to promote the circulation of data while protecting the rights and interests of data has become a hot issue in academic and judicial practice. In this regard, this paper finds the advantages of applying the anti-unfair competition law to protect enterprise data from the relevant cases of unfair competition disputes, hoping to provide useful suggestions for effectively safeguarding the rights and interests of data and facilitating the development of the digital economy.

1. Introduction

In the context of big data economy, the rapid development of digital technology and the increasing value of information resources mean that enterprises are paying more and more attention to the status of data in their strategic planning for enterprise development, and the establishment and improvement of data protection and property rights has become a key issue of concern for all walks of life. With the development of economy and science and technology, the competition for data among enterprises has become increasingly fierce, affecting the order of market competition, and the protection of the rights and interests of enterprise data has gradually become a focus of attention, all of which have posed new challenges to the existing legal system.

2. Overview of Unfair Competitive Behavior of Enterprise Data

2.1. Concepts and Basic Characteristics of Enterprise Data

Enterprise data is a collection of data with economic value that is involved in the process of collecting, mining and processing a large amount of user information for the purpose of application or transaction. As a hybrid containing many information contents, it integrates many types of data in the process of generation on the premise of enterprise holding, and it is easy to generate contradictions and conflicts between different interest subjects when utilizing and circulating.

Enterprise data can be used by many people at the same time without being affected by the use of others, with the characteristics of non-competition and non-exclusivity, which meets the core requirements of public goods in economics and has the characteristics of public goods.[1]

The scarcity of enterprise data is proposed by law, similar to intellectual property rights are not de facto scarcity. Legal protection of enterprise data is precisely to affirm the enterprise in the process of collecting, processing, organizing data to pay, incentives for enterprises to further excavate and utilize the collected data, improve the supply of data resources, and further meet the market demand for data.[2]

The holders of enterprise data are enterprises, which are economic organisations that conduct production and operation and provide products and services with the fundamental purpose of making profits. When protecting enterprise data, legislators should take into full consideration the profit-seeking nature of enterprises, and balance the interests between enterprises and enterprises, between enterprises and individuals, and between enterprises and society.

2.2. Manifestations of Unfair Competitive Behavior in Enterprise Data

This paper studies the narrowly defined unfair competition behavior in the enterprise data industry, i.e., the behavior of operators who, in the process of data acquisition, use and transaction, violate the generally accepted principles of business ethics and honesty and credit, which adversely affects the competitive interests of the data operators and the legitimate rights and interests of the data subjects, and disrupts the industry's competitive order.[3]

2.2.1. Improper access to enterprise data

Any unauthorized access to data collected and stored by other operators during the data collection phase is considered unauthorized access to enterprise data and a direct violation of data processing rules. In its raw state, this data may be technically disparate and have no economic value in isolation. However, when this data is aggregated due to economies of scale, that is, when it is aggregated from quantitative to qualitative variations, its business value increases dramatically. Because of the value and confidentiality of business data, these data must be strictly protected by law. Any access to enterprise data against the wishes of the data owner would not only violate business ethics, but also jeopardize the fairness of market competition.

2.2.2. Improper Use of Enterprise Data Behavior

Specific manifestations of the improper use of enterprise data mainly include: the use of data for competing products or services with substitution effects; and the acquisition and use of such data may harm the legitimate business interests of other organizations, or harm the security of the information network, the privacy of users, the security of personal information, and the public interests of society. The characteristics of these acts are mainly reflected in two aspects: on the one hand, relative to the data property rights and interests accumulated by the enterprise in the previous period, the actors have not paid labor for the relevant work, and the enterprise has paid a large amount of manpower, financial resources and other operating costs for the collection and collation of these data, and its rights and interests should be protected by law. Regardless of whether the network technology used by the actors is reasonable or not, it does not exempt them from the legal responsibility they must bear; on the other hand, the way in which the actors use the data has the problem of forgery and homogenization, which is sufficient to make it unnecessary for users to obtain the data from the enterprises that are in compliance with the enjoyment of the data, and the provision of this kind of content constitutes a substantial substitution that exceeds the scope of the reasonable use of the data, and in serious cases, it will disrupt the development of the data industry and the market system.

3. Enterprise Data Anti-Unfair Competition Law Protection Versus Other Paths

3.1. Criminal Law Pathway

In the “first case of criminalization of crawlers”[4], the court held that the defendant unit and the defendant violated the state regulations by using network crawler technology to invade the technical security measures of the victim company against the victim company's crawlers, and obtained the video data stored on the victim company's server, causing the victim company to lose 20,000 RMB in technical service fees, and found that the defendant unit and the defendant constituted the crime of illegally obtaining computer information system data. And the defendant constituted the crime of illegally obtaining computer information system data.

From the viewpoint of relevant provisions and judicial practice, the existing data protection mode of criminal law indirectly protects data through the protection of the computer system that operates the data, the information content carried by the data, and the virtual property credentials represented by the data. The premise of relying on criminal law for data protection is that criminal acts against data are in line with the circumstances of traditional crimes or have caused the harmful results of traditional crimes. Based on the above premise, in the era of digital economy, new types of data crimes may not be evaluated for illegality. On the one hand, the existing criminal law constrains narrower behavioral patterns and incomplete behavioral stages. The behavioral types of new data crimes such as deep counterfeiting, data blocking, and data forgery cannot fit with the existing criminal elements. On the other hand, due to the modesty of criminal law, the path of criminal law to regulate data protection may be too harsh.

3.2. Contract Law Path

When the plaintiff and defendant have a contractual relationship on the data in question, the contract agreed by both parties can be used to determine whether the acquisition and use of the relevant data is in line with the agreement between the two parties, and whether the defendant has a breach of contract liability. In the “face recognition dispute case”[5], the court ruled that the plaintiff for the defendant's annual card for the park authentication, allow the defendant to collect fingerprint information, the two sides reached an agreement; The defendant unauthorized modification of the park into face recognition, essentially modifying the agreement between the two sides, should bear the responsibility of breach of contract.

However, the premise of contract law to protect data is pre-existing expressly established or presumed to be established contractual relationship, such as the non-existence of contractual relationship that is not applicable space. Most of the viewpoints also think that the feasibility of the contract law path of enterprise data protection is not high, after all, in practice, most of the cases against the acquisition and utilization of enterprise data often come from a third party, and the business operator and the third party, a potential data violator of the contract is not concluded in advance, the contract law is difficult to third party infringement of remedies.[6]

3.3. Monopoly Law Path

When data resources become an important manifestation of an enterprise's competitiveness, the larger and richer the data resources controlled by the enterprise, the more scale effect it has. The Organization for Economic Co-operation and Development (OECD) has pointed out that the data-driven market is more concentrated and prone to monopoly than other markets. [7]Based on this, the amended Anti-Monopoly Law of the People's Republic of China of 2022 clarifies the applicability of anti-monopoly related regimes in the field of enterprise data protection and the specific rules. Among them, there are both principle-based provisions[8] and detailed rule provisions[9].

From a practical point of view, data monopolization behavior broadly includes three kinds of algorithmic conspiracy, abuse of dominant market position, and operator concentration. However, the lack of price in the data economy, the hidden and dynamic nature of algorithmic conspiracy, and the dilution of market boundaries arising from the rapid development of the market have caused the traditional paradigm of anti-monopoly analysis to be partially dysfunctional. With procedural rules such as subject qualification and jurisdictional confirmation, as well as the identification criteria for data monopolization not yet clear, the applicable rules of the antitrust law for data monopolization need to be further explored. At the same time, it is questionable whether seeking to protect one's own enterprise data in individual cases can be included in an antitrust review.

3.4. Patent Law Pathway

Data-related interests have something in common with the objects of specialized laws on intellectual property. Patent law, as one of the specialized laws on intellectual property, is also taken into account in the data protection path. However, the basic principle of patent law is “disclosure in exchange for protection”, whereas enterprise data comprises a variety of types, many of which are not publicly available and do not meet the prerequisites for the granting of patents. At the same time, most enterprise data is a collection of user information, payment information and other data, and lacks the novelty and inventiveness requirements for patenting, making it more difficult to seek relief under patent law.

3.5. Copyright Law Pathway

In practice, there are two scenarios in which enterprise data may constitute a work: firstly, with the authorization of the author, the enterprise operator claims the copyright on the relevant text, short video, art and other works produced by the users in its enterprise. Second, the business operator's processing, integration and screening of the data collection is original, and it is claimed that the database constitutes a compilation work. However, ensuring the realization of data rights and interests through the copyright system is facing three dilemmas: firstly, it is difficult to meet the standard of “originality”, which is a key element for constituting a work, and the judgment of “originality” is dependent on the judge's discretion. In the first case of legal protection of navigation electronic map data[10], the court of first instance held that the navigation electronic map in question, even if part of the data reflected a certain degree of personalized choice, was not sufficient to conclude that it enjoyed copyright over the entire map data. The court of second instance, on the other hand, held that the map in question, despite its special characteristics in terms of storage form, still belonged to the map works protected by the Copyright Law. Secondly, compared with the huge amount of enterprise data, the works authorized by the users can be said to be “a drop in the ocean”. If enterprises are required to obtain authorization from authors one by one, they need to invest high monetary costs and incalculable time costs to be protected by copyright, which is not conducive to encouraging enterprises to carry out data integration and innovation on this basis, and at the same time, when faced with some large-scale data capturing behaviors of enterprises, the Copyright Law can not play a role in protecting them either. Thirdly, if a business operator claims that a collection of data constitutes a work, it also means that he or she has accepted various restrictions and limitations such as fair use and statutory licenses as stipulated in the copyright law.

3.6. Trade Secret Path

Depending on the degree of publicity, enterprise data can be categorized into public data, which are disclosed to all without discrimination, and non-public data, which are not fully disclosed. Among them, public data do not meet the characteristics of trade secrets and cannot be protected by trade secrets. And the data is not public, the enterprise does not know whether it can be protected by trade secrets. Generally speaking, the trade secret protection approach to protect the interests of data is feasible within a certain range, but some enterprise data is public information, is the blind spot of the trade secret protection system, can not be effectively protected. Therefore, enterprise data to realize the value of data and the cooperative development of the digital economy is also difficult to be protected under this paradigm.

3.7. The Path to Unfair Competition Law Beyond Trade Secrets

Starting from the "microblogging pulse" case, which is the first case of "big data unfair competition", the path of competition law has gradually become the most popular choice for business operators to safeguard their own enterprise data from improper infringement in recent years. In such judicial decisions, the rights and interests of business operators have been vigorously defended through the negative evaluation of the improper capture and use of business data.

Currently, the anti-unfair competition law is mainly applied to protect enterprise data under Article 2 (hereinafter referred to as the General Provisions) or Article 12 (hereinafter referred to as the Internet Specific Provisions) Paragraph 2(4) of the Law, and the criticism of this path mainly lies in the controversy over the understanding and application of the specific legal provisions; the application of the abovementioned more principled provisions, the standard of "Business Ethics" or the standard of "Business Ethics" or the standard of "Business Ethics" are not applicable. When applying the above principle-based provisions, the lack of details on the standard of "business ethics" or the consequences of "disrupting the market order" creates uncertainty in the rules of adjudication; the frequent application of the general provisions or the underpinning provisions of the Internet-specific articles may lead to higher costs of data compliance, which is not conducive to the sharing of data; and the inability of business operators to claim exclusive rights through the determination of their interests in law. Exclusionary rights, etc. However, from the perspective of practical development, the multi-subjective nature of the data value chain and the plurality of interests carried make data protection need to consider the interests of multiple parties. The path of behavioral regulation by competition law is to assess behavior by integrating multiple factors in individual cases, a dynamic, scenario-based judgment method, which gives adjudicators the flexibility to respond to changes brought about by innovation and the opportunity to weigh the balance of interests. At the same time, although the protection of legitimate rights and interests by competition law is not exclusive and requires economic operators to prove the infringement of commercial rights and interests by the behaviors adopted on a case-by-case basis, it makes it possible to incorporate the anti-law into the framework of the protection of other types of rights for a trial, experimental, or transitional period first, when the specific intellectual or commercial achievements are worthy of protection, and not yet capable of constituting a right, and are not conveniently incorporated into the framework of protection of other types of rights. For this reason, under the current legal framework, the competition law route may be the best route for enterprise data protection.

4. Conclusion

With the booming of the digital economy, the role of enterprise data for operators has become increasingly important. Reasonable protection of enterprise data can promote data sharing among operators, thus encouraging more high-quality data supply for enterprise data. This paper examines the possible paths of enterprise data protection by combing and analyzing the existing judicial practice experiences. It hopes to provide judicial guidance on the protection of enterprise data pursued by business operators, as well as support for the protection of data rights and interests, further releasing the effectiveness of data elements and promoting the development of the digital economy.

References

[1] Mei, Xiaying. Between sharing and control The private law limitations and public order construction of data protection [J]. Chinese and foreign law, 2019, 31(04):855.

[2] Zhang Jianwen, Liu Xiaotian. The Governance Path of Corporate Data Disputes in the Era of Digital Economy--Centering on the Anti-Unfair Competition Law [J]. Journal of Northwestern Polytechnical University (Social Science Edition), 2023,(01):106.

[3] Song Ziwen. Research on the protection of enterprise data against unfair competition law[D]. Harbin University of Commerce, 2024.

[4] See (2017) Beijing 0108 Criminal Investigation No. 2384, which is in force.

[5] Case No. (2019) Zhejiang 0111 Civil 6971, Case No. (2020) Zhejiang 01 Civil 10940, the case was remanded for a new trial on appeal and the judgment was revised.

[6] Long Weiqiu. Revisiting the path of property rights for enterprise data protection[J]. Oriental Law, 2018, (03):50-63.

[7] Wu Changhai, ed., Data Jurisprudence, Law Press, Beijing, 1st edition, February 2022, p. 189.

[8] See Article 9 of the Anti-Monopoly Law of the People's Republic of China for details.

[9] See Article 22 of the Anti-Monopoly Law of the People's Republic of China for details.

[10] Case No. (2016) Jing 0108 Min Chu 27234, (2019) Jing 73 Min Zhong 1270, the case was remanded for a new trial on appeal and the judgment was revised.