Exploring the Legal Protection Path of Commercial Data

Xinyu Liu[1,a,*]

[1]*School of Business Administrationt, Shandong University of Finance and Economics, Jinan City, China*
a. 3176939775@qq.com
**corresponding author*

Abstract: With the rapid development of digital economy, commercial data has become the core element of enterprise competition, but its legal protection path has not yet formed a unified system.An in-depth exploration of the definition and characteristics of commercial data, analyzing the differences between it and public and corporate data, and highlighting the unique attributes of commercial data in terms of aggregation, value and dynamism are the basis for understanding its legal protection.On this basis, the existing legal protection paths are systematically sorted out, covering the paradigm of empowering legislation, anti-unfair competition law and intellectual property protection, etc. However, these paths still face many limitations in practical application, such as the tendency of pan-interventionism, the difficulty of identifying competitive relationships and the ambiguity of business ethics standards.The existence of these problems highlights the need to optimize the path of legal protection of commercial data, for which it is proposed to build a multi-level, synergistic and comprehensive protection system, optimize the application of the anti-unfair competition law, and create a dual security protection system for secret and public data through legislation. At the same time, the proposal to construct a special article on commercial data can better promote data sharing and the development of artificial intelligence.

Keywords: business data, anti-unfair competition law, business ethics, intellectual property law, digital jurisprudence

1. Introduction

1.1. Background and significance of the study

In the era of rapid development of digital economy, business data has become more and more important and has become an indispensable key element in the market. For various enterprises, business data not only affects their business model, but also relates to their advantageous position in the market competition. Business data is like a "compass" for business operations, which is indispensable for enterprises to make decisions, analyze market conditions, and develop new products. The legal protection of commercial data is also a problem. While commercial data is becoming more and more important, legal protection problems have also arisen, for example, there is not yet a clear conclusion as to what nature it actually belongs to legally; the ways to protect commercial data are also rather messy, and there is no unified system; in judicial trials, the adjudication standards of commercial data-related cases are not uniform, and different verdicts may be rendered in the same

situation. These problems have brought a lot of trouble, not only preventing commercial data from being fully utilized, but also possibly leading to negative consequences such as data monopoly and data abuse. Therefore, it is of great theoretical and practical significance to study the legal protection path of commercial data and explore suitable protection mechanisms.

1.2. Concepts and characteristics of business data

1.2.1. Definition and characterization of business data

Under the wave of digitalization, business data has become a core element of enterprise development. It is a collection of data with economic value formed after collecting, organizing and analyzing user behavior, transaction records and other information in the daily operation of enterprises.[1]Just for example, users' browsing records, social media followers, favorite products and so on. By analyzing and processing these data, enterprises can better access market demand, optimize products and services, and thus enhance competitiveness.

The characteristics of business data focus on aggregation, value and dynamism.[2]Aggregation means that business data is not a simple listing of individual pieces of data, but rather a resource that is formed when an enterprise aggregates and processes a large amount of data. These data are assembled together in order to realize greater value. Value is reflected in the fact that business data can be transformed into economic benefits in business activities. Its value stems from the application of data in actual business scenarios rather than the data itself. For example, e-commerce platforms can benefit from analyzing users' purchase data to provide merchants with precise marketing suggestions to help them increase sales. Dynamism means that business data is in a constant state of flux. The data is continuously updated as time and business progresses. Just like DDT, an online taxi platform, the data of passengers' hailing time, taxi type, payment amount, etc. are always changing. The platform allocates vehicles based on these real-time changing data to improve operational efficiency and better meet user needs.

1.2.2. Difference between commercial data and public and enterprise data

There is a clear difference between commercial data, public data and enterprise data, which play different roles in the digital economy. On the one hand, the three differ in terms of the subjects and sources to which they belong. Public data is generated by government departments in the performance of their functions, like the data recorded by water and electricity supply departments. Business data, on the other hand, is formed by enterprises in their market operation activities, such as user shopping data accumulated by e-commerce platforms. Enterprise data is divided into enterprise raw data, enterprise data products and enterprise data collection.[3]On the other hand, there are also differences among the three regarding legal positioning and protection. The protection of commercial data is controversial and is mostly based on the Anti-Unfair Competition Law, but there is a problem of inconsistent application standards in judicial practice. Public data is mainly managed according to government data management regulations, focusing on ensuring data security and reasonable use to serve the public interest. The protection of enterprise data requires comprehensive consideration of the rights and interests of enterprises, the nature of data and relevant laws and regulations, and different types of enterprise data are protected in different ways.

2. Existing paths to legal protection of commercial data and their limitations

Existing paths for the legal protection of commercial data include the empowerment legislation paradigm, the anti-unfair competition law path, and the intellectual property protection path. All of

these paths are important means of protecting commercial data, but all of them have limitations of varying degrees.

2.1. Empowering the legislative protection paradigm

The theoretical basis of the empowering legislation protection paradigm contains the theory of natural rights of labor, the theory of utilitarianism and the principle of misappropriation. In terms of the logic of application, the overall construction of the paradigm is to set the constituent elements of protected commercial data, typify and delimit infringements, and delimit the boundaries of protection, such as the model of China's Exposure Draft of Anti-counterfeiting Laws; the object of protection is "property rights and interests", which provides transitory protection of data; and data controllers provide transitional protection of the data through technological measures such as IDs, passwords, and other management measures to restrict access to data by specific people, equivalent to Japan's electromagnetic management measures. In judicial practice, this paradigm enhances the certainty of legal protection, reduces the cost of arguing the legitimacy of data rights and interests protection in individual cases, and improves the efficiency of judicial adjudication, as in the case of Weimeng v. Antfang Software Unfair Competition.

The empowering legislative protection paradigm has multiple significant limitations in commercial data protection. At the methodological level, it seriously contradicts the principle of moderation. While the core objective of the law against unfair competition is to safeguard the freedom of competition, the empowering legislative protection paradigm adopts a static and absolutist pan-interventionist approach to protection, which overly focuses on the rights and interests of data controllers and completely ignores the overall interests of market competition and the rights and interests of consumers. This "infringement" logic not only misinterprets the essence of anti-unfair competition law, but also triggers pan-interventionism and creates excessive impediments to market competition. At the level of technical tools, its theoretical foundation is flawed in many ways. The theory of natural rights of labor faces many difficult confusions when applied to commercial data. For example, the applicability of the link between labor and property to non-material objects is unclear, there is a lack of objective and uniform standards for defining labor and judging its value, and there are doubts as to whether laborers are able to acquire complete property rights in commercial data. These problems make it difficult for the theory to be a solid basis for empowering legislative protection. The application of utilitarian theory in the field of commercial data is also very limited. While the theory advocates incentivizing innovation through empowering protection, in practice, the characteristics of commercial data dictate that there is no significant incentive deficit in the market. In addition, the theory cannot effectively demonstrate whether the benefits of incentivizing innovation outweigh the costs of the incentive itself, which makes its application in practice much less valuable. The criteria for determining the doctrine of misappropriation have continued to expand and evolve in practice, from a single criterion based on the acquisition of a "quasi-property right" through labor, to a multiple criterion containing various elements, such as "time sensitivity," "free-riding representation," "existence of a direct competitive relationship," "constituting significant harm," and so on. [4]It has gradually expanded and evolved from a single criterion based on the acquisition of a "quasi-property right" through labor to a multifaceted criterion that includes various elements such as "time-sensitivity", "free-rider characterization", "existence of a direct competitive relationship" and "constituting a significant injury". However, this shift has not solved the problems of the principle in practice, such as the difficulty in accurately defining the elements of "competitive relationship" and "significant harm" emphasized by the behavior-centered determination model, which has led to a great deal of uncertainty in the specific application of the principle. . In addition, the empowering legislation protection paradigm has some specific practical problems. Firstly, it may lead to data monopolization, giving excessive power to data controllers and restricting the free flow of data and

competition, which is detrimental to both the healthy development of the market and the interests of consumers. Then excessive empowerment and protection may inhibit the innovative vitality of the market. Data controllers may shy away from sharing and utilizing data easily for fear of infringement risks, thus hindering technological innovation and business model development.

2.2. Path to protection under the Unfair Competition Law

The Unfair Competition Law indirectly protects commercial data by regulating unfair competition and plays a key role in cases such as Weibo v. Pulse. The law intervenes when an enterprise's competitive interests are jeopardized by the improper acquisition, use or disclosure of its commercial data. Its advantage lies in its high flexibility, with general provisions coupled with specific provisions that can respond to the complex and changing patterns of competition in the data field, such as emerging behaviors such as data capture and misuse, which can be judged and constrained on the basis of relevant principles even if they are not explicitly provided for in the law, providing broad legal support for the protection of commercial data.

The anti-unfair competition law has a unique role and value as an important legal tool for the protection of commercial data. By strictly regulating unfair competition, the law provides indirect protection for commercial data. Its advantage lies in its high degree of flexibility and its ability to adapt to the complex and changing circumstances in commercial data protection. Whether it is emerging data competition behavior or disputes over rights and interests that have not yet been clearly defined, the Anti-Unfair Competition Law can be adjusted through its broad provisions, providing the necessary legal basis for the protection of commercial data and effectively filling the legislative gap. However, the anti-unfair competition law has also revealed some limitations in its practical application.

Firstly, the determination of competitive relationships has become exceptionally difficult. In the traditional economy, the competitive relationship is relatively clear, and the operators are usually in the same field and provide similar products or services, so the competitive relationship is easy to judge. However, in the era of digital economy, new types of competition modes such as cross-border competition and platform competition are emerging, the boundaries between different fields are becoming blurred, and the phenomenon of industry crossover is becoming more and more obvious. For example, some enterprises seemingly unrelated to the data business may, through data mining and analysis, have a competitive relationship with data-related enterprises. This makes it difficult to apply the traditional standards for determining competitive relationships. Moreover, if the determination of competitive relationship is strictly adhered to as a precondition for the determination of unfair competition, it may lead to the determination of unfair competition too narrowly and fail to fully protect the fairness of market competition.[5]Secondly the ambiguity of business ethics standards is a prominent issue. In the emerging field of data, business ethics has not yet formed a clear and unified standard and is still in the process of continuous development and change. Business ethics is a kind of subjective value judgment, which is influenced by specific social background, economic environment and industry policies, and different people have different understanding and perception of it. This leads to the lack of a clear basis for judges to judge whether a business behavior is in line with business ethics in judicial practice, which is easily influenced by individual subjective factors, resulting in different adjudication results. For example, in certain data crawling cases, as to whether it constitutes unfair competition, different judges may make different judgments due to their different understanding of business ethics. There is also a tendency for anti-unfair competition laws to rightsize competitive interests, which also brings about a series of problems. Elevating competition interests to rights for protection tends to confuse the institutional functions of anti-unfair competition law and tort law. The purpose of the anti-unfair competition law is to maintain the order of competition in the market, not to protect the competitive interests of particular operators. However,

when competitive interests are rightsized, judges, when judging whether a competitive act is justified, tend to presuppose the legal rights and interests of the protected operator, and then make judgments based on the existence of aggravating acts and damaging consequences. This practice may lead to excessive intervention in market competition and restrict the free competition of market players. At the same time, the rightsizing of competition interests may also neglect the protection of consumer rights and interests. In commercial data competition, in order to protect their competitive interests, operators may take various measures to restrict the circulation and sharing of data, thereby jeopardizing the legitimate rights and interests of consumers, such as the right to know and the right to choose.

2.3. Pathways to intellectual property protection

Intellectual property protection is an important way to protect commercial data, including copyright protection and trade secret protection, however, they both have certain limitations. In terms of copyright protection, publicly available commercial data with a high degree of originality may be protected in accordance with the law if they meet the constitutive elements of the copyright law in terms of selection, organization or content.[6]However, not all commercial data can satisfy the originality requirement, and data that lacks innovativeness, such as the process of collecting and organizing raw data, is difficult to be covered. Moreover, although the scope of protection and the manner of exercising rights under the copyright law are clearly stipulated in the law, there may be unclear provisions for emerging forms of commercial data, which makes it difficult for right holders to defend their rights. In terms of infringement remedies, the identification of infringement and the determination of the amount of compensation are faced with a number of complex issues. Right holders need to provide sufficient evidence to prove the existence of infringement and the resulting damages. However, due to the uncertainty of the value of commercial data itself, the calculation of the amount of compensation is often difficult. In terms of trade secret protection, trade secret protection mainly targets those non-disclosable data with secret nature and commercial value, such as customer lists and technical formulas. However, due to the continuous progress of technology and the frequent movement of personnel, these secrets are easily leaked, so it is difficult to maintain the secrecy of trade secrets for a long time. Therefore, it is necessary for the right holder to take effective confidentiality measures, such as technical encryption and personnel management, etc. However, this to a certain extent restricts the right holder from giving full play to the value of the commercial data, and also hinders the circulation and utilization of the data.

3. Optimized paths for legal protection of business data

In the era of digital economy, the legal protection of commercial data needs to be improved. In this regard, we can explore the construction of a comprehensive protection path, the optimization of the protection of the anti-unfair competition law, and legislative proposals in three aspects.

3.1. Construction of an integrated conservation pathway

3.1.1. multilayered protection

In view of the complex characteristics of commercial data, a multi-level legal protection system should be constructed. Take those data products that have been processed in depth and carefully organized, and show certain creativity, they have a high degree of originality, and this kind of data collection can be prioritized for protection by copyright law. Copyright law can clearly define the ownership of such data and provide solid and powerful protection. In actual judicial practice, once the infringement of commercial data is involved and the infringement is within the scope of protection

of the copyright law, the right holder can rely on the relevant provisions of China's copyright law, such as Article 2, Article 15, Article 52, etc., as well as the "Interpretation of the Supreme People's Court on Several Issues on the Application of Law in Trial of Cases of Civil Disputes over Copyright" and other judicial interpretations, to determine the basis of their own right of action and claim damages for infringement from the infringing party. The infringing party to claim damages for copyright infringement.

On August 24, 2020, the Supreme People's Court adopted the Provisions on Several Issues Concerning the Application of Law to the Trial of Civil Cases Involving Infringement of Trade Secrets, in which "data" is explicitly listed as a kind of business information, which opens up a new avenue for data right holders to protect their data from the perspective of trade secrets. Those commercial data that cannot be disclosed, the boundary of rights and interests is fuzzy and uncertain, and often need to clarify the rights and interests with the help of external control measures, so the trade secret system, which is centered on the protection of the rights and interests of enterprises, is very suitable for coordinating this kind of situation. Trade secret protection especially emphasizes the secret status of data and the implementation of confidentiality measures, which can effectively prevent the data from being leaked or illegally used. Enterprises, as right holders, need to utilize a variety of reasonable means of confidentiality, such as strictly restricting access rights, and signing confidentiality agreements with relevant personnel, etc., to protect the security of data in all aspects.

In addition to this, there is also a large amount of general commercial data, which is neither eligible for copyright protection nor difficult to be included in the category of trade secrets. For these data, the anti-unfair competition law plays the role of underpinning protection.[7]In unfair competition disputes such as the improper use of commercial data, the parties concerned often file lawsuits on the basis of Article 2 and Article 12 of China's Anti-Unfair Competition Law. Judges often cite these provisions when deciding cases. The high-profile cases of Taobao v. Meijing Technology Company[8] and Case of Douyin v. Xiaohulu[9] are typical examples.

3.1.2. cooperative protection

In practical application, intellectual property law, contract law, tort liability law and anti-unfair competition law should be applied in concert. As a fundamental means of protection, intellectual property law provides a clear definition of property rights and a framework for the protection of commercial data. Copyright law protects the originality of data, and trade secret law protects the secrecy of data, both of which together provide comprehensive protection for the intellectual property attributes of data. Contract law ensures the legality and orderliness of data circulation by regulating data transactions and use contracts. Contract law can clarify the rights and obligations of both parties to a data transaction, regulate the authorized use of data, the duration of the license, and the liability for breach of contract, and provide legal protection for the reasonable flow of data. For example, when it comes to the signing of a contract and its performance, Article 463 and a series of subsequent articles of the Civil Code provide us with a clear legal guideline. Tort liability law can provide relief when data are infringed upon, clarifying tort liability and compensation standards. Just as Article 1165 of China's Civil Code states, "If an actor infringes on the human rights and interests of others through fault and causes damage, he or she shall be liable for tort." From the perspective of market competition order, the Anti-Unfair Competition Law carries out macro-control on the use and protection of data to prevent data monopolization and abuse. In summary, through the synergistic effect of multiple laws, an all-round and multi-level protection system for commercial data is formed.

3.2. Optimization of Unfair Competition Law Protection

3.2.1. Amendments to the determination of competitiveness

In the era of digital economy, it is difficult to adapt the criteria for recognizing traditional competitive relationships to the new mode of competition. Emerging modes such as cross-border competition and platform competition have blurred the boundaries between different fields, and the phenomenon of industry crossover has become increasingly obvious. For example, some enterprises seemingly unrelated to the data business may have a competitive relationship with data-related enterprises through data mining and analysis. Therefore, the strict determination of competitive relationship should be weakened, and competitive relationship should no longer be taken as a precondition for the determination of unfair competition. This will not only help to avoid the omission of regulation of unfair competition due to the narrow determination standard, but also protect the fairness of market competition in a more comprehensive manner.

Currently, the digital economy is developing rapidly, the data competition mode is complex and variable, and the traditional competition relationship determination standard has limitations. Weakening the determination of competitive relationship can broaden the scope of application of the anti-unfair competition law.[10]This can not only regulate emerging data competition behavior, but also resolve disputes over undefined rights and interests. In the case of data scraping behavior, for example, even if there is no traditional competitive relationship between the actor and the right holder, as long as the behavior impairs the order of competition in the market, the Anti-Unfair Competition Law can intervene to regulate it and safeguard the fairness and orderliness of the market.

3.2.2. Clarify standards of business ethics

The ambiguity of the standard of business ethics is one of the important problems faced by the anti-unfair competition law in judicial practice. In order to solve this problem, we can make use of objective standards such as industry self-regulatory conventions and technical norms to assist in the evaluation of business ethics. Industry self-regulatory conventions are usually formulated by industry associations, reflecting the generally recognized code of conduct in the industry, with strong relevance and operability. Technical regulations clarify the reasonable boundaries of data acquisition, use and sharing at the technical level, and provide a technical basis for judging whether business behavior is in line with business ethics, such as the Robots protocol used by the search engine industry to assist in evaluating business ethics.

In judicial practice, judges should construct specific rules in conjunction with objective criteria such as industry self-regulatory conventions and technical norms. For example, the judiciary has created the principle of non-interference in the public interest. In the Internet industry, when an e-commerce platform operates normally and provides users with commodity trading services, another e-commerce platform cannot, for the purpose of obtaining a competitive advantage, hijack the traffic on its platform through technical means, resulting in users being diverted to its own platform without their knowledge, and this kind of behavior violates the principle of non-interference in the public interest. These rules provide a positive and effective example for many subsequent cases, which will not only reduce the cost of market operation, but also help the courts to solve the problem of difficulties in recognizing business ethics when hearing similar cases.

With the rapid development of the digital economy, business ethics standards need to be constantly adjusted and improved. Therefore, both industry self-regulatory conventions and technical specifications as aids to evaluating business ethics should change accordingly with the rapid development of the times and technology. For example, now that artificial intelligence technology is more and more widely used in data processing, the relevant technical specifications should promptly

add the new contents of algorithmic fairness and data privacy protection, so as to ensure that the business ethics standards are always in line with the current actual situation and are truly effective.

3.3. Legislative Recommendations

3.3.1. Creating a Dual Security Protection System for Secret and Public Data

Create a dual security protection system for secret and public data, and take different protection measures for different types of data.[11]Commercial data include both secret data that need to be kept confidential and public data that can be shared openly, so the distinction between secret and public data is crucial. Secret data has value due to confidentiality, and should be included in the protection of commercial secrets; while the value of open data lies in the circulation and utilization, and should be regulated through the mechanism of data rights and interests protection. However, in the current practice in China, usually do not distinguish between open data and secret data, but both are included in the data protection. For example, in the case of "Gumi v. Yuan Guang",[12] the defendant illegally obtained data information through technical means to break the encryption system of the plaintiff. In the case of Gumi v. Yuan Guang, confidential data and information that meet the requirements for trade secret protection can be included in the protection of trade secrets.

3.3.2. Constructing a "business data bar"

At present, the "Special Article on Commercial Data" in the "Law of the People's Republic of China on the Prevention of Unfair Competition (Draft Revision for Opinion)" has preliminarily clarified the elements of the protection of public data and the types of behaviors, but it still needs to be further improved. First, the types of infringement behavior need to be further clarified. Data infringement is mostly focused on improper capture and use, and there are already conditions to sort out, summarize and typify the infringement acts identified in judicial practice. Second, the design of exemptions or fair use clauses is crucial, and sufficient space should be left for data sharing and public domain. Currently, generative artificial intelligence is developing rapidly, and the training of large models requires massive amounts of data, so in order to allow for the further development of artificial intelligence, there should be more lenient space for data acquisition and utilization.

4. Conclusion

In the era of digital economy, the path of legal protection of commercial data is characterized by diversification, and the existing empowerment legislation paradigm, the path of anti-unfair competition law and the path of intellectual property protection each have their own feasibility, but also have significant limitations. In view of these limitations, the path to optimize the legal protection of commercial data can start from the following three aspects. The first is to build a multi-level, synergistic and comprehensive protection system, combining copyright law, trade secret law and anti-unfair competition law to ensure that different types of data are appropriately protected. Second, the optimization of the anti-unfair competition law should weaken the identification of competitive relationship and clarify the standard of business ethics, so as to adapt to the new competition mode in the era of digital economy. Third, the legislative level should create a dual security protection system for secret and public data, and further improve the "special article on commercial data" to clarify the types of infringement and reasonable use provisions, so as to leave space for data sharing and the development of artificial intelligence. Through these optimization paths, the legal protection of commercial data will be more comprehensive and flexible, and better able to face future challenges.

References

[1] Liu Ying, Gao Zheng. Legislative protection of commercial data under the conceptual dichotomy of data and information[J]. Science, Technology and Law (in English and Chinese), 2022,(04):1-9+82. DOI:10.19685/j.cnki.cn11-2922/n.2022.04.001.

[2] Qiu Fu'en. Construction of Rules for the Protection of Commercial Data against Unfair Competition[J]. Intellectual Property Rights,2023,(03):77-100.

[3] Zhong Xiaowen. Theoretical Logic and Practical Architecture of Enterprise Data Titling [J]. Credit Collection, 2022(11):23-31.

[4] Shi Xinyuan. A Methodological Review of the Adjustment of Commercial Data Anti-Unfair Competition Law[J]. Nankai Journal (Philosophy and Social Science Edition),2024,(01):51-66.

[5] LIU Zhihong. Commercial data competition law protection: coupling relationship, realistic challenges and optimization scheme[J]. China Circulation Economy,2022,36(12):114-123.DOI:10.14089/j.cnki.cn11-3664/f.2022.12.010.

[6] HU Li. On the Protection Mode and Right Setting of Data Property[J]. Journal of Northeast Normal University (Philosophy and Social Science Edition),2024,(04):156-164.DOI:10.16164/j.cnki.22-1062/c.2024.04.017.

[7] Wu, Gui-De. Private Law Protection of Commercial Data and Path Selection[J]. Comparative Law Research,2023,(04):185-200.

[8] Zhejiang Provincial Higher People's Court (2019) Zhemin Shen 1209 Civil Judgment.

[9] Civil Judgment (2021) Zhe 0110 Min Chu No. 2914 by the People's Court of Yuhang District, Hangzhou City, Zhejiang Province.

[10] Li Yang,Su Yi. Rethinking and Solving the Commercial Data Protection Model[J]. Guangdong Social Science,2023,(04):255-266.

[11] Kong Xiangjun. Practical Reflection and Legislative Prospect of Commercial Data Protection: Conceptualization of Protection Path Based on Property Attributes of Data and Information[J]. Comparative Law Research, 2024,(03):72-92.

[12] Refer to Civil Judgment (2023) Jing 0102 Min Chu No. 7890 by the People's Court of Xicheng District, Beijing Municipality.