Proceedings of ICILLP 2025 Symposium: Digital Governance: Inter-Firm Coopetition and Legal Frameworks for Sustainability
DOI: 10.54254/2753-7048/2025.BR27184

Reconstruction of the Path for Commercial Data Protection: Reflections on the Existing System and Protection Path and Innovation of a New Tiered Progressive Model

Zerun Zhao

School of law, Hunan University, Changsha, China
18903158716@163.com

Abstract. As a core element of the steadily developing digital economy nowadays, the value of business data is increasingly prominent. However, at present, China has not yet formed a clear and systematic legal protection path, so the related disputes occur frequently. This article first defines the concept of commercial data and clarifies that it possesses four core attributes, then explore the limitations of the existing paths: the property rights model is prone to monopoly and ambiguity of ownership; The creditor's rights model is restricted by the relativity of the contract. The copyright model only covers data compilations with "originality". Although the Anti-Unfair Competition Law is the mainstream, its provisions on the protection of trade secrets have a narrow scope of application, and there are problems such as ambiguous standards and insufficient connection between the general provisions and the special provisions for the Internet. Based on this, this paper proposes a new tiered progressive protection model: giving priority to protecting original data under the Copyright law; Where the originality is not met but the requirements such as confidentiality are met, the protection of trade secrets shall apply. For the remaining data, the Internet Special Provisions and General Provisions of the Anti-Unfair Competition Law shall be applied in sequence. This model aims to precisely protect the rights and interests of commercial data, balance the efficiency of data circulation and the competitive order. However, its implementation still requires improving legal connections and judicial rules, etc., to provide a solid institutional guarantee for the protection and rational utilization of commercial data.

Keywords: commercial data, protection path, new tiered progression model, Copyright Law, Anti-Unfair Competition Law

1. Introduction

With the vigorous development of new-generation information technologies such as artificial intelligence and big data, the digital economy has become an important driving force for promoting social transformation and high-quality economic development. Under the conditions of the digital economy, business data is not only one of the key production factors for enterprises, but also an important business resource and competitive advantage for them [1]. The status of commercial data is on the rise, and disputes over data capture and rights infringement are constantly emerging,

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.BR27184

becoming a hot topic in current legal research. In the face of this issue, China has not yet made direct legal arrangements for data rights confirmation and data protection paths. The academic circle has discussed the direct empowerment of property rights protection model and the creation of commercial data control and usage rules for creditor's rights protection model. Both of the above protection models can seek basis in the Contract section, property rights section and tort liability section of the Civil Code. In addition, the academic community has also discussed the protection models of intellectual property law, anti-unfair competition law, and even the construction of new types of data property rights, aiming to achieve comprehensive protection of commercial data.

2. Developing a concept of commercial data

The question of "what it is" serves as a prerequisite for initiating a discussion. Therefore, before delving into the protection models for business data, it is necessary to provide a more detailed definition of its specific concepts.

2.1. Definition of commercial data

Data is a collection of information that relies on algorithmic computing power technology to present various original facts, observations or symbolic representations that describe objective things, times or phenomena in objective forms such as text, numbers, images and sounds. Article 3, Paragraph 1 of China's Data Security Law defines data as "any record of information in electronic or other forms". At present, data can be classified into personal data and non-personal data. In local legislation in cities such as Shenzhen and Shanghai, non-personal data is further divided into public data and commercial data. However, at present, there is no separate law in China that has a written definition of the concept of "commercial data". Only the "Anti-Unfair Competition Law (Draft for Comment)" of 2022 attempts to define commercial data, which stipulates in Article 18, Paragraph 1 that commercial data is "data collected by business operators in accordance with the law, which has commercial value and corresponding technical management measures have been taken". This legislative move indicates that China has included the protection of commercial data within the scope of regulation of the Anti-Unfair Competition Law, and this regulatory approach is also in line with the mainstream stance in current judicial decisions.

2.2. Eligibility criteria for commercial data rights

The concept of commercial data itself is novel and controversial, and the academic community has not yet reached a consensus on the definition of the constituent elements of its rights. Based on the definition of commercial data in Article 18 of the Anti-Unfair Competition Law (Draft for Comment), the author distills three basic constituent elements: First, it must be collected by the operator in accordance with the law; Second, it has commercial value; Third, corresponding technical management measures have been taken. Based on this, combined with the viewpoints of multiple theories, the four core legal attributes of rights-based commercial data are further summarized:

First, legality. This is the prerequisite for commercial data to be protected by law, which echoes the basic requirement of "collecting data in accordance with the law", emphasizing the compliance of the entire process of data acquisition and utilization.

Second, scale. Supported by new technologies, scattered information is integrated into large-scale data sets through algorithms and big data technologies. This is an important feature for data to

DOI: 10.54254/2753-7048/2025.BR27184

generate commercial value.

Third, manageability. This is reflected in the fact that the right holder discloses their rights claims through necessary management and protection measures, which not only confirms the basic requirement of "having taken technical management measures", but also provides an objective basis for the demarcation of rights boundaries.

Fourth, value. This is the core sign that distinguishes commercial data from public data. Article 18, Paragraph 3 of the Anti-Unfair Competition Law (Draft for Comment) clearly stipulates that data that the public can use for free does not fall under protected commercial data. Such data should be classified as public data due to the lack of exclusivity and commercial value. Article 127 of the Civil Code of the People's Republic of China provides parallel protection for data and online virtual property, which also confirms that the protected data should possess value attributes similar to those of property.

3. Multi-dimensional approaches to commercial data protection in China

Article 127 of the Civil Code on the protection of data and virtual property not only confirms that the necessity of data protection in the era of big data has been widely recognized, but also highlights that the importance of data has risen to the scope of legal protection. However, regarding the protection path of commercial data, China's legislation has not yet clearly defined specific rules, and the academic community has not reached a unified understanding either.

The academic community's exploration of the path for commercial data protection shows phased characteristics: In the early stage, the direct empowerment model of property rights protection was discussed, but at present, a few scholars still hold this view. Since then, some scholars have proposed a creditor's rights protection model, advocating that the rights and obligations of both parties in data transactions be regulated through contract law, and that tort liability law be used to make up for the damage to rights. In addition, some scholars advocate including data as intangible assets within the scope of intellectual property protection. The most mainstream judicial approach in current judicial practice is to protect commercial data through the Anti-Unfair Competition Law.

The following text will analyze the above-mentioned paths one by one from the dimensions of theoretical basis, operational cost, and protection effect, and evaluate their feasibility and potential defects.

3.1. Property rights protection model

Some scholars advocate the property rights protection model, arguing that by directly granting data property rights through the law, the regulation of the data market can be transformed from post-event relief to pre-event guidance, thus avoiding the obstruction of data circulation and market failure caused by the lag in rights protection. Its theoretical foundation is Locke's theory of labor property - under natural conditions, humans can claim ownership of common resources through labor. Extending this theory to the field of data, raw data is like natural resources. Data practitioners, by investing a great deal of human and material resources in collecting, cleaning, analyzing and processing it, endow data with economic value and thus should enjoy the corresponding property rights. This model aims to clarify data ownership, stabilize market expectations, and promote the orderly flow of data elements.

However, this model has significant limitations. Although the "intangibility" of commercial data conforms to the characteristic of "resource sharing" in Locke's theory, the exclusive rights it grants to the subjects are prone to lead to data monopolies. When rights holders restrict the use of data for

DOI: 10.54254/2753-7048/2025.BR27184

the sake of their own interests, it will create data silos, hinder the free flow and value mining of data elements, and even exacerbate the imbalance in market competition, leading to a "rights misunderstanding effect", which is contrary to the theoretical premise of "reserving sufficient resources for others". Furthermore, Locke's theory of labor property itself is facing fundamental doubts. Nozick, with the question of "Does pouring tomato juice into the sea own the entire ocean?", reveals the ambiguity of the boundary between labor and rights in this theory, that is, simple labor input does not necessarily naturally generate exclusive rights [2]. When there are logical loopholes in the theoretical foundation, the property rights protection model constructed on its basis is naturally unable to cope with the complex market practice demands. Instead, it will weaken the vitality of data innovation and intensify the risks of economic operation due to the solidification of property rights.

3.2. Creditor protection mode

The core of the creditor protection model for commercial data lies in establishing the creditor-debtor relationship among all parties through legal acts such as contractual agreements in the collection, use, and transaction of commercial data, in order to safeguard the rights and interests related to commercial data. The specific implementation path of this mode includes contractual agreements and license agreements. Among them, the contractual agreement serves as the core carrier. In scenarios such as data trading, through detailed contractual terms, the rights and obligations of the data provider and user are clearly defined, including core elements such as the scope of data usage, usage period, confidentiality obligations, and payment methods. A license agreement is similar to a contract. Data owners can issue usage licenses to specific entities, allowing them to use commercial data under certain conditions.

The normative system regarding contract formation, performance and liability for breach of contract in the Civil Code provides the fundamental legal support for this protection model. When one party to a transaction violates the contractual agreement, the other party may, in accordance with the law, claim liability for breach of contract and demand compensation for losses. In addition, this model also has the advantages of flexibility and autonomy: the parties can negotiate and determine the contract terms based on business needs, adapt to the diverse scenarios of data transactions, and conform to the principle of economic efficiency. At the same time, the relativity of contracts is conducive to clearly defining the subjects of rights and obligations, providing a clear legal basis for dispute resolution.

However, this model also has obvious limitations: First, the establishment and performance of the contract require the investment of time, energy and expenses and other costs; Secondly, in the face of complex data trading scenarios, the contract terms are difficult to cover all potential risks and are prone to legal loopholes. Thirdly, based on the relativity of contracts, it is difficult to form effective constraints and remedies for the infringement acts of third parties outside the contract.

3.3. Copyright protection model

Professional practitioners invest their labor and time in collecting, processing and handling data, ultimately producing collections of big data and data products. Rights holders can protect such intellectual achievements through the copyright protection model.

Article 15 of the Copyright Law clearly stipulates that for a compiled work to be protected by the Copyright Law, two core conditions must be met: First, the compiled object is "data or other materials that do not constitute a work"; Second, the "content selection or arrangement" of these

DOI: 10.54254/2753-7048/2025.BR27184

materials must reflect "originality". This means that for commercial data to be protected by copyright law, the key does not lie in the innovativeness of the data itself. After all, the attributes of objective data determine that it cannot be "innovated", but rather in whether data practitioners have injected unique intellectual judgment and creative labor in the content screening, structure arrangement and other links when integrating the data.

In judicial practice, In judicial practice, the court's criteria for determining this element have been clarified through typical cases. In the "Case of Clarivate Information Services (Beijing) Co., Ltd. v. Shanghai MedSci Medical Technology Co., Ltd. for Infringement of the Right of Information Network Dissemination of Works and Unfair Competition" [3], the judgment logic of the Shanghai Intellectual Property Court clearly demonstrates this train of thought: On the one hand, the IF impact factor is an objective data calculated based on a fixed formula and, due to its lack of originality, cannot independently constitute a "work". On the other hand, the JCR Journal Citation report database, after conducting research and analysis on specific topics, demonstrates a personalized judgment of "selecting the most academically valuable journals" in the journal inclusion process. The intellectual creativity in this screening process meets the requirement of "originality", thus constituting a compiled work protected by copyright law [4]. It is worth noting that although the collection of IF impact factor data in this case lacks originality in itself, it is protected by relying on the overall originality of the database as a core component of the originality database. This judgment indicates that when courts determine whether data compilations can constitute works, they always focus on whether the data screening, processing, and arrangement processes reflect "originality", rather than the attributes of the data itself.

In summary, the Copyright Law has clear boundaries for the protection of commercial data: it only applies to compiled works that meet the "originality" standard in content selection and arrangement. For data sets that do not meet this standard, even if efforts have been made, it is difficult to be included in their protection scope. However, the popularization of electronic information technology has made "data online" the norm. Raw data that has not been innovatively integrated, due to its huge scale, has gradually demonstrated significant economic value. As scholars have pointed out, the use value of data does not stem from creativity or arrangement, but from the information it carries, which makes the protection of data in the form of compiled works highly limited [5].

3.4. Protection model under the Anti-Unfair Competition Law

3.4.1. Trade secret protection model

According to Article 10, Paragraph 4 of China's Anti-Unfair Competition Law, the composition of trade secrets must meet three elements: secrecy, economic value and confidentiality. For business data that enterprises have collected, processed, organized and arranged at a huge cost and are reluctant to disclose to the public, if it meets the above conditions, it can be protected as a trade secret, thereby safeguarding the interests of the enterprise.

However, from a practical perspective, the coverage of business data by the trade secret protection model is actually limited. From the perspective of the three elements, business data usually possesses the element of "economic value", which needs no further elaboration. However, in today's digital economy environment, one of the major characteristics of all kinds of data is openness and transparency. Most of the data comes from public channels, and the cost of taking measures to encrypt and protect the data is extremely high. This makes it difficult to meet the two requirements of "secrecy" and "confidentiality", resulting in a very narrow scope of practice for this

DOI: 10.54254/2753-7048/2025.BR27184

protection model. Furthermore, if enterprises overly rely on trade secret protection mechanisms to safeguard their commercial data rights and interests, they may form "data silos" due to excessive protection and even lead to monopolies. This not only restricts the free flow of data but also goes against the original intention of commercial data protection.

3.4.2. General provisions of the Anti-Unfair Competition Law protection model

Article 2 of the Anti-Unfair Competition Law, as a general provision, offers a broader range of protection possibilities for commercial data. This clause focuses on the legitimacy judgment of market competition behaviors, with its core being to regulate behaviors that "violate the principle of good faith and business ethics, disrupt the market competition order, or damage the legitimate rights and interests of other business operators or consumers". This means that even commercial datasets that are in a public state can be regulated through this clause if others obtain or use them through improper means, and such behavior violates the generally recognized business ethics in the industry, disrupts the fair competition order or directly harms the legitimate rights and interests of the data owner.

However, this protection approach has obvious flaws: First, the legal attributes of commercial data are not clearly defined. The protection logic relies on "behavioral regulation" rather than "rights definition", which increases the difficulty for right holders to provide evidence. Secondly, there is insufficient connection with the provisions on trade secrets in Article 10 of this Law. If it constitutes a trade secret, it is likely to cause confusion in the application of the law. For public data that does not constitute trade secrets, even if others obtain and use it in bulk through technologies such as web crawlers, due to the lack of specific guidelines on the "reasonable boundaries" of data collection and use, it is easy to fall into disputes of "excessive protection" or "insufficient protection". Thirdly, it is difficult to cope with the challenges posed by technological development and new scenarios. In the digital economy, the ways of data acquisition and utilization are constantly innovating. However, the principle-based provisions of the second article are difficult to respond promptly, resulting in a lack of clear judgment standards for whether new types of data utilization behaviors that are subjectively "non-malicious" but actually harm competition constitute "violations of business ethics". This makes judicial decisions difficult to keep pace with the rhythm of technological innovation in practice.

3.4.3. Internet-specific protection model

Article field of the Internet, has established a more explicit "list of behaviors" by specifying unfair data acquisition behaviors such as "fraud, coercion, evasion or destruction of technical measures". Compared with the principle-based provisions of the second article, this clause significantly enhances the operability of judicial decisions. It no longer relies on the flexible interpretation of abstract concepts such as "business ethics", but provides judges with clearer guidance for judgment through enumerative provisions. At the same time, it lowers the threshold of evidence for rights holders, making the determination of "improper conduct" more objective.

From the perspective of the content of the provisions, the first three items of the second paragraph of Article 13 clearly list three typical types of unfair competition behaviors on the Internet: traffic hijacking, interference, and malicious incompatibility. The fourth item, on the other hand, uses a catch-all clause to deal with possible new types of behaviors in the future, forming a legislative model of "summary + listing + catch-all", which is more comprehensive than before. More importantly, this clause is dedicated to balancing the order of market competition with the efficiency of data circulation: its core is not an absolute ban on data acquisition, but rather focuses

DOI: 10.54254/2753-7048/2025.BR27184

on regulating "improper methods" and takes "legal possession of data" as the premise of protection. This setting not only reserves space for the legal sharing and reasonable use of data, but also clarifies the boundaries of rights by clearly stating that "illegally obtained data is not protected". In practice, its protection of data presents a hierarchical logic: for non-public data, if there is no cooperative relationship, the acquisition behavior often needs to be achieved through technical means that destroy or bypass access rights, and such behavior is bound to lack legitimacy. For public data, it is necessary to first review the legality of the means of data collection, and then further determine the legitimacy of subsequent usage behaviors. This hierarchical treatment to a certain extent breaks through the predicament of the general clause protection model. It not only avoids the rigid competition caused by excessive protection but also prevents the improper restrictions on the market-based circulation of data elements due to the abuse of rights, achieving a dynamic balance between the protection of operators' rights and interests and the free circulation of data.

4. New tiered progressive protection model for commercial data

Based on the above analysis of the legal protection pathways for commercial data, the author believes that a 'tiered progression' logic can be established. That is, different protection models should be applied in sequence according to the matching degree between the attribute characteristics of the data and the legal requirements, which not only ensures the accuracy of protection but also takes into account the balance between data circulation and market competition.

4.1. Priority application of Copyright Law

First, with 'originality' as the core criterion for judgment, priority should be given to considering the possibility of the application of the Copyright Law. If commercial data demonstrates the intellectual creativity of data practitioners in terms of content selection and arrangement methods, that is, such selection or arrangement is not a simple mechanical summary but incorporates unique judgment, screening logic or structural design, reaching the "originality" standard in the sense of the Copyright Law, then it can be included in the category of "compiled works" as stipulated in Article 15 of the Copyright Law Protect the legitimate rights and interests of the right holder over the data product through the copyright protection model. The reason for giving priority to this protection path is that the Copyright Law sets a clear and relatively high threshold for "originality", and the legal nature of its rights content greatly reduces the uncertainty of rights claims.

4.2. Transfer to trade secret protection

Secondly, if commercial data cannot be protected by copyright law due to a lack of "originality", it will be transferred to the review dimension of trade secret protection, with a focus on verifying whether it simultaneously meets the three requirements stipulated in the Anti-Unfair Competition Law: First, secrecy, that is, the data is in a state not known to the public and cannot be easily obtained through public channels; Second, economic value. Data must have actual or potential commercial value and be able to bring competitive advantages to the rights holders. The third is confidentiality. The right holder needs to take reasonable confidentiality measures (such as technical encryption, permission management, confidentiality agreements, etc.) to maintain the confidential state of the data. For business data that enterprises have invested a high cost in and clearly do not wish to disclose, if it does not constitute a monopoly and meets the above conditions at the same

DOI: 10.54254/2753-7048/2025.BR27184

time, they can prohibit others from obtaining, disclosing or using it through improper means through the trade secret protection model, thereby safeguarding their competitive interests.

4.3. Regulation based on anti-unfair competition regulations

Finally, when commercial data neither meets the "originality" requirement of the Copyright Law nor is it difficult to constitute a trade secret due to the lack of "secrecy" or "confidentiality", other provisions in the Anti-Unfair Competition Law can be used as further protection paths, and it is necessary to distinguish the application levels of the Internet special provisions from the general provisions. The author believes that Article 13 of the Anti-Unfair Competition Law, namely the special provisions on the Internet, should be given priority for application: This clause provides clear and definite behavioral regulation standards for the protection of public or low-secret data by listing specific improper behaviors such as "fraud, coercion, evasion or destruction of technical measures". Especially when determining the legitimacy of data acquisition means, its "behavioral list" style of provisions can reduce the reliance on abstract concepts such as "business ethics". Enhance the operability of protection. As the Internet Special Provisions still need to be further improved in judicial practice, if the alleged act does not fall within the regulatory scope of the Internet Special Provisions but indeed violates the principle of good faith and business ethics and disrupts the market competition order, the general provisions of Article 2 of this Law may be applied for supplementary regulation. By comprehensively assessing factors such as the legitimate rights and interests of the rights holders, the legitimacy of their actions, and the impact on market order, a bottom-line protection for data rights and interests is achieved.

The above-mentioned tiered progressive protection path not only respects the core elements and applicable boundaries of different legal systems, but also matches the best protection model based on the specific characteristics of commercial data such as the degree of originality, confidentiality status, and circulation demands. While avoiding the abuse of rights or malicious competition that harms the legitimate rights and interests of data practitioners, it also prevents excessive protection from hindering data circulation. Ultimately, achieve a dynamic balance between commercial data protection and the development of the digital economy.

5. Conclusion: commercial data protection effectiveness and outlook

In the future, with the deepening development of the digital economy, the ideal state of commercial data protection should be one with a clear legal framework, complete industry self-discipline, co-governance by multiple entities, and flexibility. At present, the hierarchical progressive protection model proposed by the author itself also has many problems. To truly implement it, it still needs to directly face practical challenges. In the construction of commercial data protection paths, the connection and coordination among different laws are the primary prerequisites. It is necessary to systematically sort out the provisions of relevant laws such as the Civil Code, the Copyright Law, and the Anti-Unfair Competition Law in terms of rights definition and regulation of competitive behavior, clarify their applicable scenarios and boundaries, and reduce legal application conflicts through legislative interpretation or cross-departmental coordination mechanisms, laying a unified rule foundation for judicial practice.

On this basis, in order to balance judicial efficiency and operability, institutions such as the Supreme People's Court and the Market Supervision and Administration Bureau should enhance collaboration, draw on the typical dispute handling experience accumulated in practice, and formulate and release targeted trial details, special guidelines and guiding cases for the Anti-Unfair

DOI: 10.54254/2753-7048/2025.BR27184

Competition Law in the field of commercial data [6]. On the one hand, by refining the rules and guidelines, the trial-and-error costs incurred by judicial authorities due to ambiguous legal provisions can be reduced, and the efficiency issues brought about by repeated arguments can be alleviated. On the other hand, by leveraging the standardized trial framework and the exemplary effect of typical cases, the scientific nature and authority of judicial trials can be directly enhanced. In addition, experts and scholars can also distill the rules of judgment by deeply interpreting official documents, enabling judicial organs at different regions and levels to form relatively stable judgment standards when handling similar commercial data competition cases, and ultimately build a stable and predictable judicial guarantee system for fair competition in the field of commercial data.

References

[1] Deng Shemin, Hou Yanling. The Practical Dilemmas and Solutions of Enterprise Data Competition Law Protection [J]. Science and Technology Law (Chinese and English), 2021, (05): 1-10. DOI: 10.19685/j.cnki.cn11-2922/n.2021.05.001.

[2] Liu Lin. The Rise and Critique of the Theory of Commercial Data Property Rights in the Big Data Era [J]. Journal of Huazhong University of Science and Technology (Social Sciences Edition), 2022, 36(02): 99-107. DOI: 10.19648/j.cnki.jhustss1980.2022.02.10.

[3] Beijing Internet Court Research Team. System Coordination and Rule Innovation in Judicial Protection of Data Rights Intellectual Property Rights [J]. Legal Application, 2024, (04): 102-119.

[4] Shanghai Intellectual Property Court: Judgment Document (2020) Hu 73 Min Zhong 531.

[5] Hu Li. On the Protection Model and Rights Configuration of Data Property [J]. Journal of Northeast Normal University (Philosophy and Social Sciences Edition), 2024, (04): 156-164. DOI: 10.16164/j.cnki.22-1062/c.2024.04.017.

[6] Li Yang, Su Yi. Reflections and Solutions on Commercial Data Protection Models [J]. Guangdong Social Sciences, 2023, (04): 255-266.