Proceedings of the 3rd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/181/2025.23255

Current Dilemmas and Paths to Cracking the Business Data Protection Pathway

Feiran Zhang

School of Law and Economics Administration, Wuhan Insititute of Technology, Wuhan, China
2639680029@qq.com

Abstract: Driven by cloud computing, big data and other technologies, commercial data with scale, value and intangibility are facing security risks, and the existing protection path has limited effect due to ambiguous standards and difficulties in proof, so it is necessary to build a systematic protection mechanism to protect the rights and interests of data and promote international cooperation. China's Anti-Unfair Competition Law relies on Article 2 and Article 12 for the protection of commercial data, but there are problems such as vague concepts and conflicting laws in Article 2 that lead to inconsistent adjudication standards, and problems such as unclear definitions and imbalanced burdens of proof in Article 12, which urgently need to be refined in order to build a systematic protection mechanism that is suitable for the digital era. The protection of commercial data in China is mainly protected by contract law, intellectual property law and anti-unfair competition law, but it faces the problems of difficulty in proof, ambiguous definition of technical means and restriction of the elements of competitive relationship, and it is necessary to improve the relevant rules in combination with the characteristics of commercial data. With regard to the many dilemmas faced by China's commercial data protection, it is necessary to build a systematic protection mechanism and simultaneously improve the application of the law to effectively deal with them.

Keywords: commercial data, intellectual property rights, unfair competition, data protection

1. Introduction

1.1. Presentation of the issue

With the booming development of new-generation information technologies such as cloud computing, big data, artificial intelligence, etc., the ways in which data are collected, processed and stored are becoming more and more complex and varied, and cyber-attacks are becoming a common threat, data protection is facing great risks and challenges. The rise of the digital economy has led to an increasing public awareness of data security, and society's demand for data protection has become higher and higher, with the value of data becoming more and more recognised. Protecting data is protecting value. In today's era of globalisation, data often needs to flow across national borders, and effective data protection can help promote international exchanges and cooperation and avoid friction and conflicts caused by data issues.

Protection needs based on the characteristics of commercial data itself: 1. Commercial data has a scale. Commercial data is different from fragmented individual or a very small amount of data, which

DOI: 10.54254/2754-1169/181/2025.23255

should have a certain scale.[1] That is to say, commercial data is different from fragmented data, and it should have a certain magnitude and scale.2. Commercial data has value. Commercial data should have economic value, which can bring benefits to operators.[2] As commercial data is generated in the market business activities, commercial data itself carries a unique value and contains certain economic benefits.3. Commercial data is intangible. Based on the appearance of commercial data rights can be seen, in the context of big data and cloud computing era as a civil rights object of massive commercial data in the appearance of the characteristics and rights attributes of the first performance is intangible, that is, the essence of its bearing is embodied in the form of digital information, and this information due to its special physical composition can not be directly "visible", but only through a specific physical composition.And this kind of information because of its special physical composition can not be directly "visible", but only through specific technical means, network and electronic equipment devices to make it reproduced and use. Commercial data based on computer applications, communications and other information technology, the form of its expression mainly includes graphic symbols, numbers, letters, etc., which determines the commercial data is not a tangible way of human perception, but by the intangible way of expression similar to the object works protected by copyright. Based on the characteristics of commercial data different from tangible objects and intangible intellectual property rights, as well as the actual economic value contained in itself, it has a reasonable need for protection. The current legislation in China for the protection of commercial data is not perfect, the law does not specify what kind of protection measures for commercial data can reach the reasonable degree of the law. This also makes different courts have different understanding of the legal provisions, resulting in the application of the law is very easy to bias, very easy to appear the same act of different judgements, so that the judicial authority is damaged, but also make the infringement of the opportunity to take advantage of.

Currently, the main protection paths for commercial data are the general terms protection path, the Internet-specific protection path and the trade secret protection path. Under the path of general terms protection, there is no clear standard for evaluating the legitimacy of competitive behaviours, and it is often chosen to judge competitive behaviours through business ethics. However, the definition of business ethics is relatively vague and general, making it difficult to obtain proper protection for business data. The protection of commercial data is more difficult to realise under the protection path of internet regulations. In the process of practice on the Internet special article, the Internet special article itself plays a very limited role, and the text of the provisions of the expression is also relatively vague and general, can not completely exclude acts of legitimate competition, has great limitations. Under the path of trade secret protection, it is difficult for general commercial data to be recognised as trade secrets, and it is very difficult to prove the fact of infringement of commercial data.

1.2. Definition and scope of business data

1.2.1. The concept of business data

Data is the information base based on binary strings of "0s" or "1s" in computers formed in different ways, and evolved into many different digital contents, goods and services with the help of the Internet and information technology. Business data is a relatively general concept, which includes public data, public (national) security data, commercial data, and personal information data (sets) in the form of data.[3] In addition, data can be further classified into two categories, personal data and non-personal data, depending on their usage scenarios or objects, where non-personal data can be further subdivided into public data and commercial data.

As a result, the concept of commercial data can be summarised as follows: commercial data is a collection of non-personal data with economic value, including text, graphic symbols, numbers, letters, etc., collected and compiled or processed by a commercial subject for commercial activities

DOI: 10.54254/2754-1169/181/2025.23255

based on information technology means, such as computer applications, communications and modern management technologies.

1.2.2. Conceptual discernment between commercial data and public data

Commercial data includes not only public data but also non-public data. There is a correspondence between commercial data and public data. Article 2, paragraph 4 of the Shanghai Municipal Data Regulations stipulates that public data refers to data collected and generated by government agencies, public institutions, organisations authorised by law to manage public affairs, and organisations providing public services, such as water supply, electricity supply, gas supply, and public transport, in the course of performing public administration and service functions. Public data is usually collected and generated in the performance of public administration and service tasks. Unlike public data, commercial data is a collection of data collected, processed and managed by private subjects using specific technical means. Commercial data include both raw data (collected to be used for commercial purposes) and "derived" data (further processed).

2. Our judicial practice

Although China's current Anti-Unfair Competition Law does not establish specific protection rules for the protection of commercial data, the use of the Anti-Unfair Competition Law for the protection of commercial data is the main means of commercial data protection. In our judicial practice, we mainly rely on Articles 2 and 12 of the Anti-Unfair Competition Law to provide protection for commercial data, but there are still major loopholes in the protection it provides.

2.1. No clear criteria for the application of article 2 of the law against undue competition

2.1.1. Vague definition of key concepts

Article 2(2) of China's Anti-Unfair Competition Law defines "unfair competition" as "conduct that violates the provisions of this Law, disrupts the order of market competition, and harms the legitimate rights and interests of other operators or consumers". This definition is relatively general and broad, and lacks specific types of conduct and judgement standards, which leads to excessive discretionary power of the judge, and the results are easily affected by the judge's subjective judgement, resulting in different judgments in the same case.[4] Meanwhile, according to Article 2 of the Anti-Undue Competition Law, natural persons, legal persons and unincorporated organisations engaged in the production, operation or provision of services shall comply with the law and business ethics, but the definition of business ethics has not been formulated as a clear standard. Differences in the interpretation of abstract concepts such as "business ethics" and "honesty and trustworthiness" have further aggravated the uncertainty of the applicable standards.

2.1.2. The scope of application is too narrow and there is a lack of a provision on underpinning

Article 2 of the Anti-Unfair Competition Law limits the applicable subject to operators, i.e., legal persons, other economic organisations and individuals engaged in the operation of goods or profit-making services. However, in judicial practice, unfair competition committed by non-profit organisations or unlicensed and unregulated subjects cannot be regulated, leaving a loophole in the scope of adjustment of the law. Article 2 of the Anti-Unfair Competition Law regulates 11 specific acts of unfair competition, making it difficult to cover new types of behaviour in the digital economy, while the application of Article 2 still relies on the judge's case-by-case judgement and lacks a uniform standard of discretion. Moreover, the lack of a general provision as a backstop makes it

DOI: 10.54254/2754-1169/181/2025.23255

difficult for law enforcement agencies to deal with non-enumerated behaviours in accordance with the principles of the law.

2.1.3. Intersections and conflicts with other laws

Article 2 of the Anti-Unfair Competition Law includes abuse of dominant market position, administrative monopoly and other behaviours within the scope of adjustment, but such behaviours are also subject to the regulation of the Anti-Monopoly Law, which leads to conflict in the application of the law and waste of enforcement resources. The same behaviour is regulated by two laws at the same time, and the liability provisions are different, resulting in conflicts and disputes in judicial practice. Article 2 of the Anti-Undue Competition Law limits the subject to "operators", but the Antimonopoly Law provides that the government and its departments may become the subject of liability, which is a contradiction in legal logic. In addition, Article 2 of the Anti-Unfair Competition Law and the Intellectual Property Law also have a problem of insufficient connection. According to the Anti-Unfair Competition Law, trade secrets must have "practicality", but in terms of the Intellectual Property Law, only three elements are required: "secrecy, commercial value, and confidentiality measures", which makes it impossible for research results that have not entered the practical stage to be protected, thus creating a protection gap.This makes the research results that have not entered the practical stage unable to obtain protection, thus creating a protection gap. Article 2 of the Anti-Unfair Competition Law protects unregistered trademarks through the provision of "confusion of business marks", but the protection of unregistered trademarks under the Trademark Law is limited to the situation of "having a certain influence", and there is a difference between the two in the determination criteria, which is very likely to lead to disagreement in the adjudication.

2.1.4. Lack of extraterritoriality

Article 2 of the Anti-Unfair Competition Act does not provide for extraterritorial application, making it impossible to effectively pursue responsibility for unfair competition that occurs outside China but harms the market order or the interests of enterprises in China, and making it difficult to adapt to the needs of globalised competition.

2.2. Considerable limitations in the application of section 12 of the law against undue competition

2.2.1. Problems of vague concepts and unclear boundaries

Article 12 of the Anti-Unfair Competition Law mainly targets unfair competition in the Internet field, aiming to regulate network business activities and protect fair competition. However, its provisions are also very vague and lack clear standards, leading to uncertainty in law enforcement and judicial practice. For example, the lack of clear criteria for "malicious intent" in "malicious incompatibility" makes it difficult to determine subjective intent in judicial practice. Courts may have different understandings of "malice", which may easily lead to disputes. Secondly, Article 12 of the Anti-Unfair Competition Law is unclear on the definitions of conduct and competitive relationship, which leads to the confusion of the criteria for determining conduct and competitive relationship in judicial practice, and relies on the judge's discretion in judicial decision-making, which may easily lead to different judgments in the same case. In addition, some scholars advocate the dilution of the competitive relationship element, directly to the act of illegality as the core, but the current judicial still require competitive relationship, resulting in the decision of the logical contradiction. Although the Supreme People's Court has expanded the competitive relationship to "indirect competitive relationship", the specific identification criteria are still unclear.

DOI: 10.54254/2754-1169/181/2025.23255

2.2.2. Inadequate burden of proof and legal liability

Article 12 of the Anti-Unfair Competition Law also does not specify the allocation of the burden of proof. Considering the hidden and technical nature of unfair competition on the Internet, it is often difficult for victims to obtain key evidence (e.g., background data, algorithmic logic, etc.), and if the plaintiff is required to prove that the defendant acted "maliciously" or "interfered" with the defendant's behaviour, the plaintiff has to bear the heavy burden of proof and the cost of defending its rights is high.If the plaintiff has to prove that the defendant has "malicious" or "interfering" behaviour, the plaintiff has to bear a heavier burden of proof, and the cost of defending rights is higher. In terms of legal liability, the existing fines are a limited deterrent to large Internet enterprises and lack punitive measures for persistent infringement.

2.2.3. Inability to adequately cover new types of competitive behaviour

With the continuous development of Internet technology, new types of competitive behaviours emerge one after another, and the anti-unfair competition law has a lag in regulating new types of competitive behaviours. And with data becoming the core resource of Internet competition, algorithms are becoming more and more important in Internet competition, and unfair competition in the field of data and algorithms cannot be effectively regulated.

2.2.4. Insufficient connection with international rules

In the context of globalisation, multinational enterprises may use cross-border flow of data to implement monopoly or unfair competition, while Article 12 of China's Anti-Unfair Competition Law does not address the issue of multinational enterprises circumventing regulation through offshore servers, and lacks connection with international rules, making it difficult to reconcile the conflict between data sovereignty and market competition. In addition, the internationally accepted principle of technological neutrality stresses the distinction between technological tools and abusive behaviours, but the definition of "technological means" in Article 12 of China's Anti-Unfair Competition Law is not yet clear, which is also prone to conflict with international rules.

3. Current commercial data protection path

The current path of commercial data protection in China mainly includes the path of contract law protection, the path of intellectual property law protection, and the path of anti-unfair competition law protection, etc. Among them, protection through the anti-unfair competition law is the main way to protect commercial data. Among them, the protection through the anti-unfair competition law is the main way to protect commercial data.

3.1. Path of protection under the Civil Code

According to China's Civil Code, parties are required to follow the principle of honesty and good faith in the performance of contracts and fulfil obligations such as confidentiality. This provision provides the basis for agreeing on the obligation of confidentiality of commercial data in the contract, requiring that both parties should take the initiative to protect the other party's data security in the course of co-operation.[5] The scope, duration and exceptions of confidential information can be clearly agreed upon in the contract, and the other party can be required to take reasonable measures to prevent the leakage of data and to continue to bear the obligation of confidentiality after the termination of the contract. The use of commercial data can be restricted through user agreements and licensing contracts, etc., and in the event of breach of contract, such as leaking data, exceeding

DOI: 10.54254/2754-1169/181/2025.23255

the permitted scope of use of data and failing to fulfil security obligations, the parties can pursue the breach of contract liability against the other party through the Civil Code.

3.2. Intellectual property law protection path

3.2.1. Copyright law protection

If the commercial data has considerable originality, then copyright protection can be applied to it. Firstly, if the commercial data meets the constituent elements of a work, then it can be protected as a work by applying copyright law. Secondly, even if the commercial data does not have all the constituent elements of a work, if it is produced through human intellectual labour, it can be protected by analogy with the relevant provisions of the neighbouring rights under the copyright law. Finally, if the commercial data is original in its selection and arrangement, it can be protected as a compilation work as a whole. In addition to this, the protection of commercial data under copyright law has been more widely applied globally. The relevant provisions of China's copyright law are not materially different from the contents of international rules such as the TRIPS Agreement, that is to say, the provisions of China's copyright law have a certain degree of convergence with the international rules, which better circumvents the situation of conflict of applicable laws.

3.2.2. Patent law protection

In terms of patent law protection, our patent law has very limited direct protection for business data. According to China's patent law, scientific discoveries, rules and methods of intellectual activities, business methods and mere data and data collections are not granted patents. If the commercial data is only a simple aggregation of customer information or market analyses, it cannot be protected by patents due to the lack of technical innovation. Specifically, as patents need to meet the technical requirements of inventiveness, novelty and utility, it is usually difficult to meet the conditions for granting a patent if the commercial data itself cannot be transformed into a technical solution. Moreover, the scope of protection of the patent right is limited to the content recorded in the claim, which only covers the technical features and does not involve the data content itself. If commercial data are processed through specific technologies to form an innovative programme, an invention patent may be applied for to protect the technical part, while the original data are protected as trade secrets.

3.3. Paths of protection under the anti-unfair competition law

3.3.1. General provisions of section 2 of the Anti-Unfair Competition Law

The core of the Anti-Unfair Competition Law lies in the protection of market competition. Although commercial data exists objectively, it hides great commercial value and there is an extremely close connection between it and market competition, which should be protected by the Anti-Unfair Competition Law. If others use commercial data without permission, violating the principle of good faith or business ethics, a lawsuit can be filed in accordance with Article 2 of the Anti-Unfair Competition Law. It should be noted that China's Anti-Unfair Competition Law protects the normal order of market competition, therefore, it is necessary to firmly grasp the element of "competitive relationship", and only subjects with competitive relationship can be regulated by the Anti-Unfair Competition Law.

DOI: 10.54254/2754-1169/181/2025.23255

3.3.2. Article 12 of the Anti-Unfair Competition Law, dedicated to the Internet

Article 12 of the Anti-Unfair Competition Law is specifically set up for unfair competition in the Internet field, which enumerates specific behaviours such as traffic hijacking, malicious interference, malicious incompatibility, etc., and provides a certain coverage of behaviours that impede or disrupt the normal operation of network products or services by means of a touting clause. Article 12 of the Anti-Unfair Competition Law highlights the use of "technical means", which can curb the behaviour of interfering with market competition through technical means. In judicial practice, when the court applies the special article on the Internet, it mainly examines whether the data crawling is reasonable and whether the use of technical means is justified to determine whether the specific behaviour constitutes an act of unfair competition.

3.3.3. Article 9 of the Anti-Unfair Competition Law on protection of trade secrets

China's Supreme People's Court provides a way to protect commercial data from the perspective of trade secrets. According to Article 9 of the Anti-Unfair Competition Law, commercial data needs to satisfy secrecy, value and confidentiality in order to be recognised as a trade secret. In other words, only data that meets the requirements of secrecy, value and confidentiality measures can be protected through Article 9 of the Anti-Unfair Competition Law. Secrecy means that the data is not known to the public, i.e., it is not publicly available or not generally in the possession of practitioners in the relevant field. Value means that the data has real or potential commercial value and can bring competitive advantage to the enterprise. Confidentiality means that the right holder has taken reasonable confidentiality measures. The commercial secret provisions of China's Anti-Unfair Competition Law provide strong protection for commercial data that meets the requirements, but its application relies on enterprises taking the initiative to adopt confidentiality measures and proving the confidentiality of the data, which has certain limitations in concrete practice.

4. Response to commercial data protection dilemmas

Commercial data protection in China faces multiple dilemmas, with such defects as vague rules, high threshold of proof, and insufficient coverage. In order to effectively respond to the dilemmas faced by China's commercial data protection, the coordinated governance of multiple private rights and the improvement of the application of the law are now elaborated as two aspects of the response programme.

4.1. Coordinated governance of multiple private rights

The Anti-Undue Competition Law embodies the organic unity of the protection of market competition order, consumer rights and interests, and market entities, but it also has certain drawbacks. For example, for the specific application of the Anti-Undue Competition Law, it is first necessary to retrieve whether the Anti-Undue Competition Law has explicitly enumerated the behaviours involved in the case, and if it has not explicitly enumerated them, then the general provisions of the Anti-Undue Competition Law will apply. In addition, although the Anti-Unfair Competition Law serves as the first choice for dealing with commercial data disputes, it is not the only option, let alone a panacea. The prerequisite for the application of the Anti-Unfair Competition Law is that there must be a competitive relationship between the parties, and if there is no competitive relationship between the parties, then the Anti-Unfair Competition Law will be of no use. Therefore, there is a real need to find a more reasonable and effective comprehensive protection path.

The existing protection of commercial data is often limited to the regulation of a single law, or the disorderly superposition and application of various single laws, which lacks logic. On the basis of

DOI: 10.54254/2754-1169/181/2025.23255

existing theories, this paper combines the multiple private rights attributes of commercial data itself, and proposes the idea of coordinated governance of multiple private rights of commercial data protection path, which can break through the dilemma of commercial data protection. This idea can make the protection of commercial data more systematic, so that the protection of commercial data can be carried out in a layered and orderly manner, thus getting rid of the dilemma of haphazard arrangement.

Firstly, intellectual property law is a lex specialis in relation to civil law. According to the principle that special law is superior to general law, priority should be given to the application of intellectual property law for the protection of commercial data. If the commercial data does not meet the constituent elements of the object of protection under intellectual property law, then the second step is the protection under civil law. Since in practice, most of the utilisation of commercial data is carried out through the conclusion of contracts, it is of course protected by the contractual part of the Civil Code. In addition, commercial data has a certain value, i.e. it can be protected as an object of civil rights of a property nature. In the event of infringement, the application of the Tort Liability Section of the Civil Code can also be considered to seek relief. Finally, the anti-unfair competition law can be applied to protect the interests of commercial data. This systematic protection of commercial data not only avoids overlapping protection of commercial data or conflicts in the application of the law, but also restrains the arbitrariness of judges in the application of the law in the course of judicial practice, while exhausting all ways of protecting commercial data.

4.2. Improvements in the application of the law

4.2.1. Application of the modesty principle of the general provisions

The application of the general provisions should be triggered only when the specific provisions cannot be covered and the behaviour is clearly contrary to the order of competition. The multiple impacts of the behaviour on competitors, consumers and innovation efficiency should be considered in a balanced manner in adjudication. In addition, the market should be given room for self-regulation, i.e. for competition areas where stable rules have not yet been formed, priority should be given to resolving disputes through technical standards or industry agreements, and premature legal characterisation should be avoided. Unify the scale through legislation and other means to avoid conflicting standards in the application of general provisions between the administrative and judicial authorities. Through the application of the principle of moderation in the general provisions, the conflict of values between free competition and the maintenance of order will be balanced.

4.2.2. Restricted interpretation of internet-specific articles

In terms of legislation, firstly, it is possible to typify data unfair competition behaviours, add new enumeration clauses, underlining clauses, etc., and clarify the constituent elements of data protection. Secondly, the guiding role of typical cases can be strengthened, and the core standards of data protection can be clarified through the release of typical cases by the Supreme People's Court to unify the scale of adjudication and avoid different judgements in the same case. Once again, the interface between administrative and judicial remedies can be strengthened, for example, in cases involving public interests, administrative authorities are required to first investigate and fix evidence before initiating civil litigation. Finally, it will strengthen the promotion of compatibility between the rules on cross-border data flow and the domestic system, establish a dispute resolution mechanism for cross-border data flow, and enhance China's right to speak in global data governance.

DOI: 10.54254/2754-1169/181/2025.23255

4.2.3. Clear identification of the constituent elements of trade secrets

It is clear that trade secrets must satisfy the requirements of "secrecy (non-publicity) + confidentiality (confidentiality measures)", while commercial data may cover public data but must have economic value. Refine the adjudication rules and burden of proof, can lower the threshold of proof of secrecy, apply the reversal of the burden of proof, etc., to require the infringing party to prove the legitimacy of the source of the data, to reduce the burden of proof on the right holder. In addition, serious illegal enterprises can be regulated by raising the cost of violation and increasing the flexibility of penalties. For example, a dynamic penalty mechanism can be established to impose additional daily fines on persistent infringers who refuse to correct their behaviour.

5. Conclusion

In the context of the globalisation of the digital economy, commercial data is facing legal protection dilemmas such as the security risk of cross-border flow, and the existing protection paths are difficult to effectively respond to the challenges of data infringement due to the ambiguity of the standards and the difficulty of proof. In order to cope with the multiple dilemmas facing the protection of commercial data in China, we can consider giving priority to the protection of original data by intellectual property law, followed by the application of the contract or tort liability part of the civil law to restrain the use of behaviour, and finally the use of anti-discrimination law to regulate the disorder of competition; and simultaneously improve the application of law by moderately using the general terms and conditions, limiting the interpretation of the Internet article and clarifying the elements of trade secrets, optimising the rules of proof, and strengthening the interface of cross-border data governance. In order to solve the problems of difficulty in proving evidence, ambiguous technical definitions and conflicting international rules, a layered governance programme has been adopted.

References

[1] *Shi Xinyuan.(2024)A Methodological Review of the Adjustment of Commercial Data Anti-Unfair Competition Law.Nankai Journal (Philosophy and Social Science Edition),1,51-66.*

[2] *Liu Xiaoyan,Chen Hongxi.(2023)Mode Selection and Rule Optimisation of Anti-Unfair Competition Law Protection of Commercial Data.Credit,41(08),33-40.*

[3] *WU Guide.(2023)Private Law Protection of Commercial Data and Path Selection.Comparative Law Researc h,4,185-200.*

[4] *Li Yang,Su Yi.(2023)Rethinking and solving the commercial data protection model.Guangdong Social Scienc e,4,255-266.*

[5] *Hu Li.(2024)On the Protection Mode and Right Setting of Data Property.Journal of Northeast Normal University (Philosophy and Social Science Edition),4,156-164.DOI:10.16164/j.cnki.22-1062/c.2024.04.017.*