

The Dilemma and Optimization of Commercial Data Protection under the Anti-Unfair Competition Law

Kaijun Zhuang

*School of Law, Jiangsu University, Zhenjiang, China
212358440@qq.com*

Abstract. In this context of the growing importance of digital economy, business intelligence is becoming an increasingly valuable resource for companies, making its protection under the law ever more crucial. Present problems with the Anti-Unfair Competition Law are among erroneous judgments as to whether a given act is unfair or not if applied to the general provision, blurred lines between what is ethical and unethical business practices, challenges to define the extent of regulation under internet specific provisions and vague standards as to what is considered a trade secret. To improve the regulation of unfair competition over commercial data and protect corporate data rights, it is necessary to improve the protection of commercial data under competition laws by clarifying the scope of general provisions, clarifying some of the language in the online related provisions and the requirements that must be met to prove a misappropriation of a trade secret, which would help clarify how companies can secure their confidential information.

Keywords: Commercial Data, Anti-Unfair Competition Law, Legal Protection, Unfair Competition

1. Introduction

1.1. Research background

Alongside with the fast growing of digital economy, data plays an important role in driving the economic and social development and the competition between companies to acquire data is becoming fiercer. Commercial data is gradually becoming one of the most valuable assets of a company. These problems of legal protection have attracted much attention, but the current Anti-Unfair Competition Law(2019) is mainly about unfair competition behavior in physical things and conventional service field. However, the non-exclusive and replicable nature of data renders this legal framework insufficiently applicable [1]. As a result, new types of anticompetitive behavior such as data scraping and data theft has flourished and continually upended the marketplace. At the same time, data generation and usage techniques are constantly evolving, so competition becomes more complicated and hidden, such as data scraping frequently uses automatic access technologies and data misappropriation utilizes technological means to circumvent regulation, which makes it difficult to identify those activities. In short, the AUCL (2019), in terms of regulation content and elements, is still unclear about what needs to be regulated, and it has difficulty responding to

changes in the practice of data competition. In practice, when assessing if novel types of data-based competition fall foul of this principle, courts will usually refer to applicable paragraphs in the AUCL. However, the absence of clear guidance results in disparate adjudication standards that diminish court efficiencies as well as increase the risk of legal exposure for companies. The new amendment adds to the "Internet-specific provisions" a prohibition against "data scraping" as well as "abusing platform rules". Whether such provisions will have much effect is an open question. On the international front, major national information markets have developed, in some cases over many years, laws protecting the privacy of personal information traded commercially, either by statute or case law. For example, by improving flows of data across member states and protecting data rights with the new Digital Market Act and Data Governance Act, while in the United States, commercial data is protected by the California Consumer Privacy Act and through common law precedent protecting trade secrets.

1.2. Significance of the research

The research has important theoretical significance to promote the perfection of the theory system of unfair competition law and provides some new ideas in basic theories, particularly with regard to the implementation of general provisions, as well as the definition of business ethics. At the same time, through a systematic analysis of deficiencies in current law, it also gives us some foundation to propose that we need more robust laws protecting commercial information, which can help the legislation more closely meet the needs for digital economy growth. In addition, the research also has important pragmatic value. The results can be used at a legislative level to guide legislators on how they may improve the Internet-specific provisions among others so that the provisions are more operable and applicable. At the judicial level, it can provide clear guidelines for the application of the law for adjudication activities, reduce the differences in the adjudication caused by vague rules, and improve the uniformity of judicial recognition. For enterprises, the legal risks faced in the process of data development and utilization urgently need to be regulated through clear rules, which can enhance the expected stability and behavioral compliance of market entities. For law enforcement departments, more specific judgment can also be obtained when investigating and dealing with unfair competition in data. It is conducive to improving the efficiency and accuracy of law enforcement, thus promoting the legal flow and value release of data elements.

2. Overview of commercial data protection under the Anti-Unfair Competition Law

In order to better carry out research, we should first clarify the concept and legal attributes of commercial data, judicially define the unfair competition of commercial data, and make a reasonable explanation of the anti-law protection of commercial data as well.

2.1. Conceptual definition and legal attributes of commercial data

Generally speaking, commercial data are all the sets of data collected, treated or sorted out in course of companies' activities which have potentially an economical interest. It concerns not only primary data but also secondary data derived from the treatment of algorithms. In terms of law, data collections are valuable not so much for any particular data element but more generally because they have scale effects and associations. They are nonoriginal, not reproducible and collective, hence it is difficult to apply the IP protection regime on them [2].

The legal properties of business information have complicated features. On the one hand, since it is an intangible asset, it has property qualities that can bring about a company's competitiveness and economic profits. But on the other hand, the generation of data is often tied up with the rights and interest of more than one party, such as data generators, processors and users, resulting in confused boundaries of rights. To accommodate this tension between these two principles, the common law has increasingly resorted to unfair competition doctrines instead of more conventional notions of property protection for protecting commercial data, and it does so because that is where such data are uniquely situated legally. Moreover, the law treats various forms of business information differently, raw data versus derivative data are fundamentally distinct from one another both in terms of substance and foundation for legal protection. Deeply processed data sets which are subject to algorithms, because of the greater level of human creativity involved in creating them and the more complex techniques used in their creation, often are compilations or trade secrets. Alternatively, unprocessed raw data could be subject merely to property rights and contract rights. In addition, commercial data containing personal information shall be subject to additional requirements provided for in the Personal Data Protection Act. In determining ownership, both personal information rights and data property rights must be considered, further highlighting the complexity of defining the legal attributes of commercial data.

2.2. Judicial definition of unfair competition in commercial data

The standards used to determine anticompetitive conduct with respect to business information vary from case to case, and are often updated, a trend that is inevitably related to the vigorous development of the digital economy, with typical examples such as illegal mining and scraping of business data sets formed by large investments of human or material resources or circumventing by any means, including technical protection measures, the application of those restrictions on access. Such behaviors do not only directly infringe upon the legitimate rights and interests of data rights holders, but more seriously, such behaviors have disturbed the healthy and orderly competitive order of the market. As far as the comprehensive evaluation of the nature of the act is concerned, what are generally considered to be three factors that a court would examine in deciding any particular case—its moral wrongfulness as an action, its pecuniary loss, and causation in fact between the act and the injury.

From this, we see that recent jurisprudence is showing signs of evolution, shifting away from an initial strict interpretation for protection to looking at balancing interest between both parties. Balancing the legitimate rights and interests of the holder of data while courts have started to acknowledge and appreciate the intrinsic circulatory value and importance of data sharing, some decisions even creatively establish the standard of "significant substitution". This means that only when the alleged conduct genuinely creates a substantial market substitution effect for the original data product does it constitute unfair competition in the legal sense. This shift in judicial philosophy profoundly reflects the legal community's deep exploration of achieving the optimal balance between data protection and data utilization against the backdrop of the digital economy's rapid advancement.

There is still some variation among the courts in their application of standards for determining whether or not they will hear and decide particular cases. For example, some courts apply more generally applicable rules developed pursuant to Article 2 of the Anti-Unfair Competition Law, predominantly based on principles of good faith and commonly recognized standards of business ethics for making decisions [3]. However, other courts are more familiar with a direct application of the provisions contained in Article 12 of the Law that explicitly deal with acts of unfair competition

in the Internet sphere or Section 9 for misappropriation of a trade secret [4]. Such disparity between different courts' standard naturally leads to lower degree of legal certainty, while at same time creates difficulty on companies' side with their data governance and protection practices.

2.3. Reasoned interpretation of the protection of commercial data under the Anti-Unfair Competition Law

The Anti-Unfair Competition Law protects business information from a conduct control perspective. During the course of the data factor marketization, the law uses its prudential orientation to prevent possible monopoly in data due to too much power, and protect the market order for normal data flows through restriction on abusive behavior, thus achieving a balance between the rights of the controller of personal data and social interest.

On the side of the law's coherence, AUL can be seen to work well together with other laws that already protect business information. In contrast to these laws (such as the Copyright Act), which merely protects original data expressions, or the Contract Law, which only binds particular counterparties, the Anti-Unfair Competition Law offers wider avenues of relief. Its broad wording allows it to evolve with new ways that competition might manifest itself in the digital space, thus leaving necessary discretion to the practice of judges. In emergent fields, like in data scraping or data misappropriation, the Act is especially flexible and comprehensive.

Judicial practice shows that, under the premise of relying on the two criteria standards of "damage plus unfairness", the Anti-Unfair Competition Law has laid a good judicial basis to solve the dispute over business data. In the process of judging business data-related cases, courts look at more than just the amount of damage actually inflicted upon a data controller as a result of unfair competition and engage in more than mere formality regarding whether or not the alleged acts were legitimate. These assessments tend to take into account many factors such as business model innovation, consumer welfare, and market competition order to avoid instituting the rigidity of a single model of rights protection.

From the perspective of motivation, the protection action of the Anti-Unfair Competition Law helps to promote the optimal allocation of data resources. By effectively stopping improper acts such as hitchhiking and destroying technical measures, it not only ensures that data controllers get reasonable returns on the cost of data collection and processing, but also ensures the opportunity for other operators to obtain. This balanced protection mechanism helps to form a virtuous cycle of data development ecology, promoting the value realization and value-added process of data elements.

3. The dilemma and causes of commercial data protection under the Anti-Unfair Competition Law

The provisions of the Anti-Unfair Competition Law (2019) that protect commercial data are mainly Article 2, the general clause. Article 9, the trade secret clause and Article 12, the special article on the Internet. However, in the current judicial practice, these three provisions have certain difficulties in protecting commercial data.

3.1. The dilemma and causes of applying general terms

3.1.1. Misconceptions exist regarding the determination of illegitimacy

As it happens in modern practice, this assessment is usually formalistic and focuses on surface features of the conduct rather than assessing whether any actual harm was done to competition. For

example, some decisions identify acts like web scraping with unfair competition without undertaking a detailed examination of where permissible activity ends or considers neither the fact that gathering information is technologically neutral nor the beneficial aspect of data flows for fostering competitive markets. At the same time, a too expansive view of competition leads to a misunderstanding that will also capture uses and disclosures of information by parties who are not even competitors [5]. In reality, determining competitive relationships in the data sphere should be grounded in substantive conflicts of interest rather than simplistic comparisons of industry or business model similarities. In employing these catch-all sections, courts occasionally diverge from Congress's purposes in the AUCPA, labeling problems that ought to be solved by other law means as unfair competition. As the new type of production factors, data must be afforded a form of legal protection which balances the need to prevent the disordered acquisition of data from infringing on valid corporate rights with an overprotective regime which erects barriers for data access. The "one size fits all" nature of many court decisions does not take into consideration differences among various kinds of data and treating private as well as publicly available information in the same manner, some decisions have incorrectly drawn a line between invention and injurious competition, over-broadly condemning legitimate technological spidering practices to anticompetitive conduct and stifling innovation in the data economy.

3.1.2. Ambiguity and overgeneralization in defining business ethics

Since it serves as a reference point for defining generic principles stipulated by the Act on Prevention of Unfair Commercial Practices, there is an indeterminacy regarding the scope and understanding of the notion of fair trade practice which may be regarded as the foundation of this act. It follows that when deciding unfair competition claims concerning commercial data, judges frequently encounter great variation in the outcomes of comparable cases—especially in nascent areas like data scraping and use. The rules are not consistent and often call for discretionary application according to abstractions: certain decisions have tended to extend the meaning of morality in trade, directly labeling conduct like violations of trade usage or technical standards as unfair competition, which easily gives rise to unpredictability in the law and inconsistency on standards [6]. Meanwhile, there is a trend of "moral generalization" in judicial practice, which means incorporating behaviors belonging to other types of law into the evaluation system for commercial ethics and causing over-intervention through ant-unfair-competition laws in normal market competitions.

3.1.3. Uncertainty and overreach in judicial application

In the application of these general clauses in court cases, various judges have applied varied meanings to terms like "business ethics" or "good faith" resulting in wildly varying outcomes in comparable cases, and relevant companies are forced to pay increased compliance costs in order to deal with the uncertainty, indirectly undermining the predictive guidance role which the statute ought to play. Meanwhile, there are also courts over-relying on principles-based provisions when no specific provision is available to include issues that shall be regulated through market mechanism as well within the scope of law which disrupts regular operation of markets and improperly restricts business freedom. Although the open-ended nature of the principles-based provisions can regulate new unfair competitive practices, it also enables subjectively discretionary adjudication.

3.2. The dilemma and causes of applying special provisions to the internet

The Article 12 of the Anti-Unfair Competition Law (2019) adopts an enumerative method coupled with an all-inclusive rule as a legislative strategy for classifying typical unfair competition acts on the Internet, but it remains problematic when applied to the context of commercial data. The residual clause, "any other act impairing or interfering with the normal operation of a network product or service lawfully offered by another operator," is unclear and thus leaves ample room for judicial discretion as to what constitutes an illegal act under this clause [7]. This uncertainty not only leads to potentially contradictory rulings on similar cases across different courts but also directly undermines the uniformity of legal application, weakening market entities' reasonable expectations regarding the legal consequences of their actions.

From the perspective of legislative technology, there is a problem that the regulation of commercial data-related behavior in this article is unclear. The elements such as "without the consent of other operators" and "malicious" adopted in the provisions lack specific measures, and the description of behavioral characteristics such as "obstruction and destruction" fails to fully consider the specificity of some data competition scenarios. This legislative ambiguity forces judicial practice to supplement the application of general provisions, but instead weakens the institutional function of the Internet as a special provision. For example, in data capture cases, in order to comprehensively evaluate multiple factors, the court often needs to independently build a judgment framework. The judgment result is largely subject to the judge's personal cognition.

The deeper problem is that the Internet special article fails to fully reflect the competitive characteristics of the data-driven market. The traditional unfair competition behavior identification model is difficult to fit the complexity of competition in the data field, especially in key areas that balance data accessibility and data protection needs. The clause mainly focuses on the direct damage to the interests of operators, but ignores the need to coordinate user rights and interests, innovation incentives and other diversified values. The limitation of this regulatory perspective has led to the fact that the Internet special article is stretched to the limit in the face of new competitive models such as data aggregation and data analysis. It is unable to effectively regulate the data utilization behaviors that formally conform to the principle of technological neutrality but essentially undermine the order of competition.

In addition, the old-fashioned and strict interpretation of the relationship of competition in judicial decisions have also limited the actual effect of the Internet-specific provisions. The conventional determination of unfair competition usually requires that there be a direct competitive relationship between operators. But competition is also manifested more generally in data markets as inter-sector and across-platform fights over data assets, with competitive interactions having clear indirect, multi-way properties. In deciding these cases, courts often find themselves in a quandary as to whether they should expand the definition of relevant competition: applying only traditional notions of direct competition risks leaving behind new manifestations of data unfair competition that are not captured under those definitions. at the same time, as it may be accused with over-regulation and intervention in markets. In light of this difficulty, courts have taken an extremely conservative, even conservative, way to apply the Internet specific-provisions. they increasingly resort to other avenues for redress in cases involving data conflicts and thus diminish even more their operational value.

3.3. Challenges and causes in the application of trade secret clauses

3.3.1. The determination of trade secrets is subject to dispute

The standards that courts have used in applying these tests are varied. For example, there is no uniform standard on how a court should determine if business information meets the "not widely known to others outside the company" test. Some courts are more permissive and hold that information qualifies as a trade secret merely because the information is processed in any way or has an organization [8]. Others are more stringent, demanding that the data show clear originality and non-obviousness [9]. This lack of uniformity in judicial standards leads to starkly contrasting rulings in similar cases, undermining the stability of legal expectations and complicating the formulation of corporate data protection strategies. Simultaneously, disputes persist regarding the essential element of "confidentiality measures," with significant variations in how different courts define what constitutes reasonable confidentiality obligations in terms of technical safeguards and management arrangements.

At present, data collection faces unique problems in seeking trade secret protection. Even if a single data point is public information, whether the overall database formed by systematic collection, arrangement and analysis has secret attributes is ambiguous in judicial determination. Because data can be updated over time, it is not straightforward to specify at which moment confidentiality holds, raising new questions as to whether an ever-changing database may continually qualify under the "not generally known to the public" criterion. In the big data age, the diversification of the source material, makes it even harder to answer such a question. In cases where data are a mix of publicly available and non-publicly available sources, it is often unclear in court proceedings whether or not the composite constitutes a trade secret.

Second, the burden of proof in a case of trade secret infringement makes proving infringement difficult. The holder of the right must prove that the data meets all of the requirements of statute and that the infringer acquired or disclosed it by improper means a double test which is overburdening. Particularly difficult is proving this where infringers use technical means to secretly acquire the data, preventing right-holders from obtaining proof of infringement firsthand. Some courts have tried to reduce that burden, either through a lower evidentiary threshold or application of rules for shifting the burden of proof. However, this approach raises concerns about potentially expanding the scope of trade secret protection beyond appropriate limits.

3.3.2. Data trade secret infringement tends to be highly covert

Infringement of data that are claimed to be trade secrets displays unique features of secrecy compared with classic trade secrets. In order to steal data on the internet and in computer systems, infringers usually resort to technological methods including web crawlers, API interface abuse and data scraper. This enables them to obtain data sources without leaving a trail of breadcrumbs behind it, and the piracy operation has obvious cyberspace features, making it very difficult to ascertain precisely what did happen. In parallel, electronic data can also readily be altered or deleted entirely, making it difficult, if not impossible, to return it to its original condition; or creating difficulties in showing a causal connection between the violation and the injury suffered as a result of the violation. Secondly, there is often a delay in realizing the economic benefit of a data trade secret. There could be a long period of time between when the breach occurred and when the loss was realized and such delay in time also contributes to concealment of the offense.

4. Optimizing the protection of commercial data under the Anti-Unfair Competition Law

To address the challenges currently faced in judicial practice when applying the Anti-Unfair Competition Law to protect commercial data, the following three optimization pathways are proposed.

4.1. Clarify the rules governing the application of general provisions

To achieve uniformity in judicial standards, it is necessary to establish a three-tiered review framework in judicial practice. First, examine whether the relevant conduct violates the principle of good faith; second, assess whether it contravenes generally accepted standards of business ethics; and finally, determine whether it causes substantial harm to the legitimate rights and interests of other operators or consumers. By adopting this tiered framework for adjudication, judicial arbitrariness in the adjudication process can be effectively prevented, providing clear judicial guidance for the proper resolution of commercial data disputes.

When it comes to the definition of business ethics, the Supreme People's Court can clarify the judgment standards of business ethics under different application scenarios by issuing guiding cases. In response to the frequent acts of unfair competition such as data theft, the legislature has formulated more operational specific identification guidelines. At the same time, it is very important to introduce the "substantive substitution" standard to determine the legitimacy of data use, that is, when the defendant's unauthorized use effectively replaces the data products or services provided by the plaintiff, it can usually be judged that it constitutes unfair competition.

Judicial authorities shall exercise the utmost caution when invoking general provisions and strictly adhere to the principle of restraint. General provisions may only serve as supplementary regulatory bases when specific provisions are demonstrably incapable of covering newly emerging patterns of unfair competition.

4.2. Further specify the content provisions of the internet-specific clause

Article 12 of the Anti-Unfair Competition Law (2019) enumerates certain unfair competition practices in the internet sphere but has yet to provide specific regulations for emerging behaviors such as data theft. The newly revised Anti-Unfair Competition Law (2025) clarifies in Article 13(2) that the previously vague term "technical means" now refers to "data and algorithms, technologies, platform rules, etc" and introduces new prohibitions against "data scraping" and "abuse of platform rules" This affirms the legal status of legitimate data assets acquired by operators, establishing the internet-specific provisions as a comprehensive domain-specific regulation covering all unfair competition practices in the internet environment beyond those specifically enumerated in Chapter II. However, Article 13 of the newly revised 2025 Anti-Unfair Competition Law still suffers from deficiencies in comprehensively covering emerging practices and regulatory gaps. Furthermore, the boundaries of the catch-all provision remain unclear, failing to fully resolve the issue of inconsistent standards applied by different courts during practical enforcement.

In terms of legislation, the relevant provisions of the Internet special articles should be further concretized. The legislative experience of relevant foreign laws such as the EU Digital Market Law should be drawn to formulate detailed norms for key elements such as data access rights and data use conditions. In the face of platform data governance, we should further clarify the boundaries of the rights and obligations of data controllers. It helps to prevent the formation of data monopolies and safeguard the legitimate rights and interests of data investors.

In judicial practice, typified adjudication guidelines should be constructed, and differentiated judgment criteria should be adopted for different data application scenarios. For example, for public data, the criterion of "substantial substitution" judgment can be applied. When processing non-public data, it is necessary to focus on the invalidity of breakthrough technical measures.

4.3. Refine the criteria for determining trade secret infringement

At the legislative level, it is necessary to clarify the core elements of determining that data constitutes trade secrets, especially to refine the requirements for the identification of "confidential measures" in the law. It can also make a more in-depth explanation of the connotation of confidentiality and secrecy through judicial interpretation, so as to provide a clear and operable basis for adjudication for courts at all levels. Due to the differences in the security needs of data at different stages of the life cycle, it is necessary to establish a dynamic evaluation mechanism to reduce the compliance burden of small and medium-sized enterprises in terms of business data. At the same time, the threshold for identifying secrecy and confidentiality should not be set too high. Although this issue is still controversial, for the data obtained and integrated by enterprises from the public domain, as long as the results formed in the process of information collection, processing, screening and combination themselves are not directly accessible, it can be determined that they have undisclosed attributes without considering whether the original source of the data is public information.

At the level of judicial practice, there is an urgent need to establish uniform rules for the allocation of the burden of proof. Given the covert nature of data infringement, the initial burden of proof on rights holders may be appropriately reduced. When a rights holder demonstrates that reasonable confidentiality measures have been implemented and that the defendant had the potential to access the disputed data, the burden of proof should shift to the defendant. For acts of illegally obtaining data, a "presumption of infringement" rule should be introduced, compelling the defendant to prove the legitimacy of their data sources.

5. Conclusion

The current AUL does not appear adequate in order to regulate new forms of competition with data since jurisprudence demonstrates a confusing application of the general provisions and a vague definition of fair trade, resulting in a variety of unintended consequences, and ambiguity as to whether or not an activity falls within the regulatory purview of the Internet-only sections reduces predictability. Likewise, trade secret laws cannot address the more surreptitious type of infringement, such as industrial espionage. These problems, on one hand, undermine the normal utilization of enterprise commercial information and on the other hand impede the vitality development of cyberspace market innovation. Standardizing the usage principles of general provision, clarifying applicable rules of the Internet-specific provisions, and clarifying standards to determine what constitutes a trade secret will go far in creating a stronger commercial data privacy regime. On the other hand, regulation should not stifle competition nor limit innovation and economic growth by overburdening or restricting the flow of data. Indeed, implementation steps are not well established yet.

References

- [1] Liu Xiaoyan, Chen Hongqian. Model Selection and Rule Optimization for Commercial Data Protection under the Anti-Unfair Competition Law [J]. Credit Reference, 2023, 41(08): 33-40.

- [2] Ye Yinyin. Study on the Protection of Commercial Data under the Anti-Unfair Competition Law [D]. North China University of Technology, 2025.
- [3] Beijing Intellectual Property Court (2021) Jing 73 Min Zhong No. 1011; Guangdong Higher People's Court (2022) Yue Min Zhong No. 4541.
- [4] Beijing Intellectual Property Court (2019) Jing 73 Min Zhong 2799; Hangzhou Railway Transport Court, Zhejiang Province (2019) Zhe 8601 Min Chu 1987.
- [5] Wu Weiguang. Critique and Reconstruction of the Concept of Competitive Relationship in the Anti-Unfair Competition Law: A Perspective Based on the Systematic Understanding of Legislative Purpose, Business Ethics, and Competitive Relationship [J]. *Contemporary Jurisprudence*, 2019, (01): 132-139.
- [6] Supreme People's Court Case No. (2024) Zui Gao Fa Min Zai 224: Determining the act of free-riding on another's well-known trade name as a violation of industry practices constitutes unfair competition.
- [7] Fu Jianjing. Determination of Unfair Competition in the Provision of Third-Party Auxiliary Software [J]. *Journal of Henan Agricultural and Economic University*, 2021, (02): 70-76.
- [8] Shanghai No. 2 Intermediate People's Court (2023) Hu 02 Min Zhong No. 11028.
- [9] Shenzhen Intermediate People's Court (2022) Yue 03 Min Zhong No. 4682.