Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 19, No. 3, 2025

Determination of the Legitimacy of The Source of Commercial Data in The Anti-Unfair Competition Law

Kaixi Zheng *

School of Intellectual Property, Nanjing University of Science and Technology, Nanjing, China
* **Corresponding author**: Kaixi Zheng (Email: zhengkaixi0301@163.com)

Abstract: In the Anti-Unfair Competition Law (Draft for Public Comments) 2022, the special article on commercial data clarifies the basic connotation and scope of protection of commercial data in terms of forward definition and reverse division. It not only requires that it has a legitimate source, economic value, and corresponding technical management measures, but also limits the scope of data and information that do not fall within the scope of data and information that can be utilized by the public without compensation. The principle of triple authorization is used for user authorization in disputes over unfair competition of commercial data, but the principle has the problems of ambiguity of the applicable object and limitation of the applicable scope. Most of the commercial data comes from the authorization of users, so the review of user authorization is an important way to grasp the legal source of commercial data. At the same time, the controller of commercial data can, if necessary, prove to the court the legitimacy and reasonableness of the source of the data on the basis of legitimate means of access other than user authorization.

Keywords: Commercial data; Legitimate sources; Triple authorization principle; User authorization.

1. Introduction

The State Council, in the "14th Five-Year Plan for the Development of the Digital Economy" and the "Comprehensive Reform Pilot Overall Programme for the Market-based Allocation of Factors", encourages the use of the economic value of commercial data, and promotes the circulation and realization of the value of data. At the same time, the Supreme People's Court and the State Administration for Market Supervision are also looking to make a breakthrough in legislation on unfair competition in relation to commercial data. The Provisions on Prohibition of Unfair Competition on the Internet (Public Consultation Draft) also provide for data-related unfair competition.2021 Article 26 of the Interpretation of Certain Issues Concerning the Application of< the Law of the People's Republic of China Against Unfair Competition> (Public Consultation Draft) also provides for "substantial substitution" and "lawful and proportionate application". Article 26 of the Interpretation of Certain Issues Concerning the Application of the Law of the People's Republic of China on Unfair Competition (Draft for Public Comments) also regulates the fair use of commercial data from the perspectives of "substantial substitution" and "lawful and proportionate application. Although the content of Article 26 was deleted when the judicial interpretation was finally promulgated. However, the draft also reflects the legislature's reflection on the lack of legal regulation of unfair competition in commercial data.

As typical property data, it is generally recognized that commercial data are not personally proprietary. In unfair competition disputes, the existence of commercial data is also usually in the form of a collection of several or numerous data entries rather than a single or small number of data entries. Article 18 of the Anti-Unfair Competition Law (Draft for Public Comments) clarifies for the first time the connotation of commercial data, i.e., data operated by an operator in accordance with the law, with commercial value, and for which corresponding technical management measures have been taken. The definition of commercial data starts from its basic characteristics and centers around the value, confidentiality and legality of the data... The protection of commercial data under the Anti-Unfair Competition Law (Draft for Public Comments) is based on the legality of the source, but the judicial interpretation at the end of 2022 does not provide a timely answer to the question of how to recognize the legal source of commercial data. At present, judicial decisions are mainly made through the triple authorization principle of "user authorization + platform authorization + user authorization". Academics and practitioners have not conducted research on how to review user authorization. Based on this, this paper discusses the dilemma of the legitimacy of commercial data and the corresponding solution path through the defective application of the triple authorization principle of the anti-unfair competition law.

2. Difficulties in the Judicial Determination of The Use of Commercial Data for Unfair Competition

The protection of commercial data rights and interests is based on the legality of the source of the data and the appropriateness of the object of protection. In arguing whether commercial data can become an eligible object, the court usually adopts the principle of triple authorization, i.e., determining whether the source of commercial data is lawful by means of "user authorization + platform authorization + user authorization". In Taobao v. Meijing Unfair Competition Dispute, the court relied on the principle of triple authorization and held that the use of a third party should be authorized by the user to authorize the network service provider, and then also need to be authorized by the platform and the user. The Privacy Policy between Taobao and its users set out the specifics of the authorized use of users' personal information. This principle also served as the basis for the

judge's finding that the commercial data had a protected interest under competition law.

However, the principle of triple authorization itself has certain limitations. From the premise of application, the principle of triple authorization should be based on the data acquisition method specifically based on the OpenAPI cooperation mode or through other legally authorized channels. The principle of triple authorization cannot be applied to the situation where the crawling object is derived data, so the commercial data crawled by the crawler does not belong to the scope of adjustment. If the user agrees to the platform to disclose his data to the public after authorizing the platform, can the third party accept this implied consent? After all, the rights to process and collect raw data enjoyed by the platform are derived from the user's authorization and permission. If the user allows the third party to access the raw data by means of a personal license, can the third party circumvent the platform's restrictions on the raw data by relying on the collection of data obtained by the third party under such a personal license? These questions arise from the ambiguity of who the triple-authorization principle applies to. It is not clear whether the scope of data regulated by the principle includes derivative data. Therefore, in the absence of a clear interpretation of the principle of triple authorization, the adjudicator can only make a comprehensive determination of whether the source of the data is of legitimate origin in combination with other acts.

3. Theoretical Basis for The Determination of The Legitimacy of Commercial Data Sources

The first step in the judicial determination of unfair competition disputes over commercial data is usually to clarify whether the right holder has a protective interest in the commercial data. In addition to its commercial value, whether the commercial data was collected in accordance with the law is also an important reference factor. If the means of acquisition is not lawful, whether the commercial data collected by labor is protectable. On this issue, there are only two main arguments in practice: the labor production theory and the fruit of the poisonous tree theory. The former emphasizes the exchange of rights and interests in the collection process, while the latter emphasizes a healthy ecological environment for the circulation and protection of commercial data.

3.1. Theory of Labor Production

To the extent that the basis of an interest in commercial data should be based on the payment of labor, its advocates primarily cite Locke's labor theory of production. In his book, The Politics, Locke articulated the labor theory of property rights, which states that "as soon as any man makes any thing out of the state in which it naturally stands, he has mixed his labor into it, and then it is owned by that laborer." The theory holds that through long-term inputs and operations, business operators put their data through reasonable analysis and processing, so the final collection of business data obtained from should be the result of the cohesion of physical and intellectual labor. Supported by the labor production theory, the legal rights and interests of commercial data are based on both ethical and economic aspects. From the ethical point of view, the labor production theory embodies the respect for what makes a person a human being; from the economic point of view, the operating costs and technical input of commercial data are quite profitable compared to traditional industries.

The labor production theory emphasizes the cost of the price paid by business operators to produce and maintain business data, while ignoring the legality and legitimacy of the labor act itself. If the act is malicious and illegal, can labor for an improper purpose also be recognized by the law? Professor Cui Guobin argues that the basic elements for a collection of open data to be protected include the collector paying a substantial cost of collection, without regard to the legality of the data collection behavior. Although this view does not directly affirm the basis of data legitimacy, it suggests that the starting point for the rights and interests of data protection should be the substantial labor cost input. From the existing judicial cases, it can be concluded that, whether from the legislative logic or policy orientation, a single emphasis on the importance of data collection behavior and processing behavior will inevitably lead to low-cost data crawling behavior. In order to build a favorable data economy ecosystem, commercial data protection should take the legitimate source as the starting and ending point.

3.2. The Fruit of the Poisonous Tree Theory

The Fruit of the Poisonous Tree theory, which originated in the United States, first referred to evidence obtained by illegal means in the course of an investigation. If the source of the evidence is contaminated, then any evidence obtained from it is also contaminated, i.e., the evidence will not be admitted in the course of subsequent litigation. The application of the fruit of the poisonous tree theory in the field of intellectual property is not uncommon. For example, in the judicial practice of copyright, if the plaintiff's work does not conform to the originality of copyright, then it cannot constitute a work of art within the meaning of the copyright law, and the protection of rights cannot be claimed on that basis.

In terms of constituent elements, most of the commercial data belongs to the collection of data obtained by algorithmic computation of personal information. The provisions on the security protection of personal information are an important manifestation of the application of the theory of the fruit of the poisonous tree to data and information. Article 111 of the Civil Code of the People's Republic of China on the protection of personal information reads, "The personal information of natural persons shall be protected by law. Any organization or individual who needs to obtain another person's personal information shall obtain it in accordance with the law and ensure the security of the information, and shall not illegally collect, use, process or transmit another person's personal information." Although the Anti-Unfair Competition Law does not directly use "obtaining in accordance with law" as a prerequisite for data protection, it is possible to refer to the Personal Information Protection Law's provision on the legality of the acquisition of personal information due to the high degree of similarity between data and personal information in terms of both form and content. This provision indicates that commercial data has a legitimate source after authorization by the user, and the legitimate source is an important basis for the protection of platform data. As an eligible object for protection, commercial data should be a collection of large-scale data formed legally and information such as technical data and operational data for which management measures have been taken.

The use of data is closely related to the acquisition of data, and if the acquisition is not justified, the use of data is often

judged to be unjustified. The theory of the fruit of the poisonous tree also exists in the court's discussion, as in the "microblogging v. Ant Square unfair competition case," the decision document reads, "because Ant Square's behavior of capturing and storing the microblogging platform data is not legitimate, so its subsequent use of this part of the data for the eagle system to display and analyze the data does not have the basis of legitimacy because the source of the data is not legitimate. The act of using it does not have the basis of legitimacy because the source of the data is not legitimate." In reality, the court did not separately discuss the data acquisition behavior and data application behavior in the case, but uniformly evaluated the impropriety of the behavior. In the newly revised Article on Commercial Data, the protection of commercial data is limited to "obtained in accordance with the law", which is an important manifestation of the inclusion of the theory of the fruit of the poisonous tree in the protection of commercial data.

4. Principles for Determining the Legitimacy of Commercial Data Sources and Their Application

The examination of the source of commercial data is a necessary means of confirming the legitimacy of the source. The necessity of its existence includes the following two aspects: first, the security of commercial data is related to personal information security and even national economic security. Commercial data can be subdivided into different industrial parts, and data brushing, data crawling and data crashing in different industries not only harm the restrictive management measures set up by business operators, but also bring the risk of data information leakage. Secondly, the existence form of commercial data is mainly a collection of data. The protection of original data and derived data is also different. Therefore, in the trial of unfair competition disputes over commercial data, different types of commercial data are subject to different levels of scrutiny and scope of protection.

4.1. Interpretation of the Principle of Triple Authorization

The principle of triple authorization refers to the fact that data can only be acquired or captured by other technical means after three permits of user authorization, platform authorization and user authorization. The principle of triple authorization is essentially to balance the security of static data and the commercial value of dynamic data, i.e., after the platform obtains the user data, it also needs to obtain the user's authorization again based on clarifying the use of the data.

There is no disagreement in the academic understanding of the principle of triple authorization that the data acquirer should first commercial data should be acquired to the user's authorization. But there are different views on the authorization of the latter two. Mr. Wang Liming believes that the first time if the data collector must obtain authorization when collecting information, the second time to share the collected information needs to obtain another authorization (data sharing and personal information protection), that is, the subject of the latter two authorizations should be the right holder of the information. Mr. Xue Jun, on the other hand, believes that the other two authorizations are the third party's authorization from the platform and the platform's permission for the third party to use the data subject to the user's authorization. The difference between these two views lies in whether it is the platform or the third party using the data that ultimately needs to obtain the user's authorization. Mr. Li proposed that the latter two authorizations should be that the platform should obtain the user's authorization to collect the data and the third party should obtain the platform's authorization to use the data. However, it can be seen from the elaboration of the principle of triple authorization in the adjudication documents that the court is biased towards Mr. Xue Jun's view on the authorization of the latter two. Undoubtedly, the platform party that obtains the user's original data should obtain the user's authorization when sharing the data. The issue of attribution of the rights to the derived data in commercial data can be based on the labor production theory, so from the perspective of the application of the theory, Mr. Li An's viewpoint is more in line with the user's right to know about the use of the data after authorization. However, at the beginning of the application of the principle of triple authorization, the court only focused on the basic framework of labor empowerment, but neglected the scope of application of the principle of triple authorization, i.e., whether the derivative data can be subjected to the principle of triple authorization in the same way as the original data is still an unanswered question.

The principle of triple authorization is a high standard requirement for enterprises to obtain data. Since the platform has the reasonableness and legitimacy to obtain the original data, both user information and enterprise data are well protected. The principle of triple authorization eliminates legal risks between users and enterprises to a certain extent, and facilitates the process of exchange and circulation of personal information and business data. High standards of data acquisition may hinder the circulation of data and affect the traffic realization of enterprises holding commercial data. Mr. Xu Wei also believes that it is inappropriate to apply the principle of triple authorization to all types of data, and that business-to-business data access rules should be constructed typologically depending on the type of data. Mr. Liu Hui suggests establishing reasonable data flow authorization rules from the perspectives of both data types and applicable scenarios to reach the coordination between data private right protection and data public interest. The principle of triple authorization determines the basic relationship between users, data controllers and third parties in the process of data circulation, and defines the boundaries of reasonable application more clearly, which not only can be beneficial to the circulation of data and information, but also becomes an important weapon used by enterprises to protect their databases.

4.2. Specific Application of The Principle of Triple Authorization

Over the past two decades, the legislation on competition law in the field of data has been in a relative lagging state, and as a result, judicial creations similar to the "principle of triple authorization" have frequently appeared in cases of unfair competition in commercial data. Strictly speaking, the principle of triple authorization is not a general principle in the legal sense, but a legal rule with specific content.

4.2.1. Weibo v. Pulse for Unfair Competition

The principle of triple authorization was explicitly applied for the first time in the civil judgment of the second instance of Weibo v. Pulse Unfair Competition. In the second trial, both parties acknowledged that the forms of obtaining data on the Internet included obtaining data under legal authorization

and obtaining data by means of crawlers. The defendant based on the "Developer Agreement" signed by the two parties to put forward a defense, that is, based on the OpenAPI cooperation with the plaintiff, through the plaintiff authorized open API interface access. However, the court held that under the OpenAPI development model, the data provider needed to obtain user authorization for the data as a prerequisite for opening it to the third party; the third party needed to obtain authorization from the data provider to obtain the data; and finally the third party applying the user's information needed to notify the user of the purpose, manner and scope of use, and again obtain consent. Therefore, the court formed a triple authorization principle of "user authorization + platform authorization + user authorization" in the final trial.

4.2.2. Taobao v. Meijing Unfair Competition

Taobao v. Meijing Unfair Competition is the first case in China on the legal attributes and rights of big data products. Taobao's "Business Counselor" big data products are trend charts and rankings that provide some reference to the commercial activities of product purchasers, and can bring Taobao direct operating income. The Defendant argued that the Taobao User Agreement's license for Taobao to use the data was invalid, but the Court found that the Plaintiff's access to the data was reasonable and justified in light of the agreements in the Taobao Platform Service Agreement, Taobao's Legal Notices and Privacy Policy, and Tmall.com's Privacy Policy. Referring to the principle of triple authorization, the court held that a data product using user information collected by another network operator should not only obtain authorization from the other network operator, but also obtain the authorized consent of the provider of that information. As a third party, the plaintiff's use of Taobao's data should also comply with the triple authorization principle of "user authorizes platform + platform authorizes third party + user authorizes third party".

4.2.3. Qihoo v. Baidu Unfair Competition

Crawler technology itself belongs to a neutral technology, the use of crawler technology has the potential to achieve both technological innovation, but also may bring about the consequences of data handling damage. Therefore, from the legal level, the crawler agreement, a similar gentleman's agreement, does not have the formal justification of the principle of triple authorization. The judgment in this case focuses on the content not of the principle of triple authorization, but the use of the crawler agreement to carry out the use of industry practices to carry out data unfair competition. This use of raw data to produce derivative data is distinguishable from reliance on contractual provisions and industry standard practices, and the analysis of taking advantage of neutral technology cannot simply be omitted. Similarly, there are other cases where the content of the original data has not been changed, but is still recognized as constituting unfair competition, such as "Weimeng v. Cloud Intelligence Case of Unfair Competition" in which the defendant did not change the content of microblogging, and the user can still see the dynamics of the celebrity's microblogging. The principle of triple authorization has shortcomings in the application of cases that use crawler technology to obtain commercial data, and needs to be combined with other elements.

Combined with the application of the principle of triple authorization in the above three cases, it can be seen that the principle of triple authorization is not universally applicable, and its application should be premised on the premise that the data in question was obtained through OpenAPI-based cooperation or other lawful means, rather than network crawling. In addition, the court did not specify whether derivative data was included when applying the principle of triple authorization. When the crawling object is derivative data, the principle of triple authorization will be difficult to apply.

5. Summary

Despite the limitations of the application of the principle of triple authorization, the first "user authorization" insisted on by the principle of triple authorization undoubtedly strengthens the protection of personal information and commercial data. There is no uniform basis for adjudicating cases of unfair competition in commercial data, but the legal source of data also lays an important cornerstone for the protection of data rights and interests. Whether it is the legal authorization of the original data or the crawling of data, the data collector can only obtain the authorization of the user before claiming rights against the data collection in its possession. User authorization as the legal source of data has the characteristic of clear traceability.

5.1. Review of User Authorizations

From the point of view of the flow of data, commercial data is similar to intellectual property rights or other legitimate legal interests. Any form of flow should have a clear procedure for authorization. The original data authorized by the user is usually able to obtain a collection of desensitized data that is different from the original data after the algorithmic operation. From a legal point of view, user authorization of commercial data is actually closely related to personal information authorization. According to the provisions on personal information and data protection in the Data Security Law, the Network Security Law, and the Personal Information Protection Law, the use of a user's personal information by a data collector must be authorized by the user.

The Anti-Unfair Competition Law is committed to maintaining a benign market competition order and a balanced relationship between various interests. Neither the Exposure Draft nor the Judicial Interpretation contains provisions on the review of the legality of the source of commercial data. Therefore, regarding the review of user authorization in commercial data, it can be suggested to refer to the review of personal information protection. This is due to the fact that most of the commercial data can be traced back to the user authorization agreement and privacy policy established with the platform when the user logs in to the platform. As stated in the Personal Information Protection Law regarding the "notification and consent" obligations of information processors, the subject of the personal information informs the data collector of the name, contact information, purpose of processing, method of processing, and type of personal information, and obtains the individual's separate consent. At the same time, it is necessary to obtain the authorization of the individual to process and utilize personal information for the purpose, manner, type, time and place of storage, and sharing of such information. Therefore, violation of the above provisions can be regarded as an infringement of the rights of citizens' personal information in the process of information processing, i.e., the source of the data does not have legitimacy. Meanwhile, from the point of view of the subject of user authorization review, analogous to

the data and information available for trading, the value attribute of commercial data itself determines that it can be reviewed by data exchanges or other institutions with the ability to trace the source of the data. Here, reference can be made to the provisions of Article 33 of the Cybersecurity Law, which stipulates that the controller of commercial data providing data flow services shall require the data provider to state the source of the data to review the identities of both parties to the transaction, and keep records of the review and transaction. Finally, the review on user authorization in commercial data can also be qualified by local legislative norms. Shanghai Data Regulations on the legitimacy of the data is further limited to provide that natural persons, legal persons and unincorporated organizations on their legally obtained data, can be used and processed in accordance with the law. Except as otherwise provided by laws and administrative regulations or agreed by the parties.

In conjunction with the above two cases on triple authorization, it is clear that user authorization cannot be reviewed without an electronic agreement or other form of consent between the user and the data collector. A common form is the privacy policy on personal information, which focuses on whether there are rules on the use of personal information from the original collection of business data; whether users are reminded to read them in an obvious way; whether business services are refused if users do not agree to the collection of unnecessary personal information; whether the purpose, manner, and scope of the collection of personal information from third parties commissioned by the company, or from embedded third-party codes or plug-ins, are listed; and whether effective correction, deletion of personal information and user account correction are provided. The purpose, method, and scope of the collection and use of personal information by third parties or embedded third-party codes or plug-ins are listed; and whether functions such as effective correction, deletion of personal information, and cancellation of user accounts are provided. The above privacy policy indicates the limited and reasonable nature of the acquisition of personal information, and in judicial practice, it is often an important piece of evidence for right holders to prove themselves.

Whether for publicly collected, self-produced or directly collected data and information, it is necessary to strengthen the review of user authorization. At present, the Anti-Unfair Competition Law and judicial interpretations do not provide for user authorization of commercial data. Taking into account the legislative purpose of the Anti-Unfair Competition Law and the formal requirements of the legal norms, it is not a good solution to specify the review of the legality of the source of commercial data in the said legal norms. The review of user authorization also needs to be combined with the provisions of the Personal Information Protection Law on the protection of personal information. The verification of personal information for special types of data information, such as financial accounts, personal health or personal information of minors under the age of 14, needs to be separately distinguished from general information. For the collection of business data and information, attention should be paid to whether it involves intellectual property content such as trade secrets or proprietary information, and the review should focus on confidentiality agreements, prohibitions on practice, and written agreements on authorization by the corporate body, in addition to user authorization. User authorization of commercial data is an important basis for the legitimacy of data sources. Just as the definition of commercial data in the Exposure Draft of the Anti-Unfair Competition Law, data collected in accordance with the law can not only determine the reasonable boundaries of the protection of commercial data, but also provide traceable evidence for the subsequent circulation of commercial data.

5.2. Determination of the Legitimacy of The Means of Access to Data Other Than That Authorized by The User

Not all subjects of data authorization are users of the platform, and therefore other data source pathways need to be considered when exploring the legitimacy of commercial data sources. In addition to user authorization, legitimate data sources include publicly collected data information, data produced by enterprises themselves, and reasonable use of personal information portability rights.

5.2.1. Information on publicly collected data

Publicly collected data information includes open data information obtained through shared channels and open data obtained through crawler software. Open data is absolutely public and public interest, and anyone can access and use open data unconditionally. According to the third paragraph of the special article on commercial data, "the acquisition, use or disclosure of the same data as the information available to the public without compensation does not constitute the improper acquisition or use of other operators' commercial data as referred to in the first paragraph of this article". Therefore, the data that the public can obtain at will and utilize without compensation does not fall within the scope of commercial data. However, not all open data can be excluded in accordance with the provisions of the third paragraph. The determination of data and information opened by the government in accordance with the law will focus on whether the data and information can be shared. The latter is often obtained by violating a website's robots agreement or IP address. Therefore, in a judicial determination, the data must be subjected to strict compliance scrutiny. As mentioned above, data exchanges or other organizations that are capable of conducting compliance reviews of data information may conduct a traceability review of data information obtained by crawling, focusing on whether the crawler software and crawling behavior are compliant, the compliance of the crawled content, and the compliance of the crawled use.

5.2.2. Data produced by the enterprise itself

Data produced by the enterprise itself refers specifically to data and information generated internally by the enterprise in the course of its operation and production. This behavior is internal to the enterprise, so it does not involve the issue of user authorization or third-party authorization. Raw data is usually processed by certain algorithms and then traded with third parties by means of databases or API interfaces. According to different types of data, the court should respectively require the enterprise to provide supporting documents with different proving power, such as database model, logs of operation and maintenance, etc. for operational data. Since the collection of data does not involve other subjects, the analysis of data produced by an enterprise on its own needs to be comprehensively determined whether it has independent data sources, whether it categorizes enterprise data according to different sensitivity levels and other influencing factors, and whether it provides sufficiently

strong means of protection and storage.

5.2.3. Fair use of the right to portability of personal information

The right to portability of personal information refers to the right of an individual to request a processor of personal information to transfer personal information to an established processor of personal information. The content, application and scope of application of the right to portability of personal information are more clearly defined in the EU General Data Protection Regulation. It was not until the Personal Information Protection Law that the right to portability of personal information was established in general terms in the form of legal norms, and in recent years, defendants have begun to use the right to portability as a major defense in disputes over unfair competition over commercial data. In Weibo v. Headline Unfair Competition Dispute and Tencent v. Jutongke Unfair Competition, the defendants raised the defense of data portability. At that time, the court rejected the defendant's defense mainly on the grounds that China had not yet introduced the right to data portability and that the conditions for the application of the right to data portability did not meet the circumstances of the case. However, since the implementation of the Personal Information Protection Act in November 2021, the right to data portability under Article 45(3) has provided defendants with a defense. If the judiciary maintains a positive attitude towards the flow of data, then finding the optimal conditions for the application of the "right to data portability" in disputes over unfair competition of commercial data will become an important guide for data users to seek economic efficiency and avoid legal risks. The defendant can argue from the perspective of the plaintiff's users' separate authorization, the data in question belongs to the original collection of commercial data, the data in question is a reasonable use and does not obviously undermine the competitive advantage, and the use of the act of bringing convenience to consumers.

However, the "right to data portability" defense is not an absolute application. The right to personal data portability is mainly applicable to data provided by individuals, and has limited application to other data and derived data. The transfer of raw, unalgorithmically processed data by users to other platforms does not jeopardize the interests of the original data collector. From the perspective of cost, the derivative data obtained by the data collector through the algorithm does not directly become the data information held by other platforms, and the mandatory constraints on the behavior of the user rather impede the flow of data information. Therefore, from the perspective of determination, attention should be paid to whether the data information belongs to the original data, and whether the way of data transfer belongs to separate information rather than a collection of data. At the same time, it is also necessary to consider the specific circumstances of the case. Since the amount of data information to which the right to personal information portability applies does not constitute a large collection of data, the subject of the defense, the subjective state of mind, as well as the actual damage and the risk of damage caused by the application of the "right to data portability" should be taken into full consideration. When the subject is an individual and the data is not used for commercial or other economic purposes, the defense of the right to data portability may be asserted in individual cases when the risk of damage is not significant.

References

[1] Cui Guobin. Object elements of legal protection of public data collections [J]. Intellectual Property Rights, 2022, (04):18-53.

[2] Kong Xiangjun. Commercial data rights: a new type of industrial property rights in the digital age--three principles of attribution and tenure definition of industrial property rights [J]. Comparative Law Research, 2022, (01):83-100.

[3] Wang Liming. Data sharing and personal information protection [J]. Modern Law, 2019, 41(01):45-57.

[4] Li An. Legal boundaries of data competition behavior in the era of artificial intelligence [J]. Technology and law, 2019, (01):61-70.

[5] Xu Wei. Reflection on the "triple authorization principle" and typology construction of enterprise data access [J]. Jiao Tong University Law, 2019, (04):20-39.

[6] Liu Hui. The Conflict and Adjustment between the Right to Personal Data Portability and the "Triple Authorization Principle" of Corporate Data Acquisition [J]. Politics and Law, 2022, (07):114 -131.