Advances in Politics and Economics
ISSN 2576-1382 (Print) ISSN 2576-1390 (Online)
Vol. 5, No. 3, 2022
www.scholink.org/ojs/index.php/ape

Original Paper

Platform Data Protection from the Competition Law Perspective Based on Specific Conduct and Data Types

YiLong Li[1]

[1] Southwest Minzu University, Chengdu, China

Received: July 10, 2022 Accepted: August 21, 2022 Online Published: August 23, 2022

doi:10.22158/ape.v5n3p117 URL: http://dx.doi.org/10.22158/ape.v5n3p117

Abstract

In the era of big data, data has gradually become an important commercial resource in the development of the emerging economy. Under the background of frequent disputes over unfair network competition, emerging data rights and interests can be better defined and better protected from the perspective of the Competition Law. When judging whether the conduct is an unfair competition conduct, the performance of the accused conduct and the type of the data involved in the case should be accurately defined, so as to define its legitimacy.

Keywords

competition law, platform data, legitimacy, data capture and use, public data

1. Background to the Issue

With the advent of the big data era, the value of "data" has gradually been highlighted and emphasized, and the "right to data" may also become a trend. At present, data is mainly generated and applied in the Internet, and is collected and integrated with the aid of new technologies or based on new business models. Therefore, for the market players, especially the network operators who rely on traffic for their survival, the data in the platform is the information asset and important business resource for them to maintain an advantage in the competition, and to expand their businesses. Therefore, the acquisition and use of data has become the cause of frequent disputes between network operators. How to protect the data rights and interests of the operators in the network competition environment without impeding the realization of the spirit of the Internet, that is, interconnection and sharing of data, has also become a problem of widespread concern in the industry.

2. Platform Data Has the Nature of Property, and the Collecting Enterprise Has the Property Right Thereto

2.1 Lawful Factual Conduct

According to the law, the collection of personal data by the data enterprises shall be deemed as lawful factual conduct. The purpose, method and scope of the collection and use of information are expressly stated in public rules for collection and use by the data enterprises, and the consent of the data owners is obtained. The dataset formed by the collection of countless personal data becomes a new object of civil rights. For example, a civil subject lawfully constructs a house and obtains the ownership of the house once the house construction is completed.

2.2 Cost and Fairness Principle

The data controller provides a platform for data collection and traceability, such as a shopping website platform, on which the data subjects can browse and shop. The data controller and the data subject jointly participate in the data production process. In the case of Beijing Guang vs Shanghai Bancai, the court held that the data and derivative products on the platform were accumulated through a long period of operation through the plaintiff's investment of manpower, materials and financial resources. The said data and derivative products include the commercial interest of the platform enterprises and reflect their market competitive advantages, i.e. they have competitive property rights and interests.

3. Platform Data Protection under the Competition Law Path

The Civil Law cannot accurately classify platform data as a specific civil right; therefore, the copyright protection model is out of line with the actual situation. Therefore, under the circumstance that it is difficult for both the Civil Law and the Copyright Law to achieve ideal protection for data in platform, the anti-unfair competition rules which take into account the protection of competition order, operators' rights and interests and consumers' interests can better play the role of adjusting and protecting platform data.

3.1 Possibility of Application of the Anti-Unfair Competition Law to Protection of Platform Data

Competitive relationship is a prerequisite element to be considered when applying the Anti-unfair Competition Law. As data has become the basic resources of the information society, the use of data has a very wide scope. Therefore, in practice, although market entities involved in data disputes are often not engaged in the same type of or similar business activities, as long as there exists the possibility of the growth or weakening of such business elements as network user groups, it will be deemed that there is a competitive relationship between the two parties. In the case of a dispute over the unfair competition in data information on Dianping, the Pudong Court held upon trial that in the field of internet, even if the two parties have different operation modes, as long as they are competing for the same group of internet users, a competitive relationship can be determined.

Of course, considerations concerning a competitive relationship do not necessarily require that the user groups of both parties grow at the same time. It is possible that the user groups of both parties are

growing at the same time. However, if one party inappropriately uses the business resources of the other party and causes damage to the legitimate business interests of the other party, it may also be deemed that a competitive relationship exists, so that there is room for the application of the Anti-Unfair Competition Law.

3.2 Alternative Protection Paths under the Anti-Unfair Competition Law Framework

Under the framework of the existing Anti-unfair Competition Law, there are three paths for data protection: First, trade secret protection, but combining with the core element of "confidentiality" of trade secrets, only undisclosed data in the platform may use this path; for the large amount of front-end disclosed data, it is difficult to identify it as trade secrets. Second, the protection is provided by the newly added Article 12 (hereinafter referred to as the "Internet special provisions") of the existing Anti-unfair Competition Law. This provision is a specific clause regulating improper network competition behaviors. The platform data grabbing and use that impede or destroy the products or services of network operators can be included in this clause for adjustment, so that the data protection needs of operators can be relatively fully covered and the data competition behaviors of other operators can be regulated. Third, the protection provided by Article 2 of the existing Anti-unfair Competition Law (hereinafter referred to as the "principle clause"), that is, although the "Internet special provisions" cannot be applied because they do not impede or damage others' network products or services, when there are inappropriate behaviors, the application of this Article may be considered to regulate behaviors that violate the principle of good faith and business ethics.

In view of the limitations of the above first way for data protection, before the introduction of the existing Anti-unfair Competition Law, the court mainly protected platform data through the above third way. For example, in the "Pulse" case, the first data competition dispute in China, and the case of Dianping v. Baidu (the map data grabbing and use dispute), both quoted the "principle clause" to adjust the indicted behaviors. However, under the current circumstances that the "Internet special provisions" are sufficient to regulate network competition behaviors involving data grabbing and use, and the application of the "principle clause" shall follow the principle of prudence and modesty. This article believes that if the indicted behavior meets the elements of the behavior regulated by the "Internet special provisions", the "Internet special provisions" shall be applied to regulate data competition behaviors, so as to better respond to the expectations of network operators on data protection and regulate the current order of data competition. Of course, based on the "Internet special provisions", there shall be behavior that destroys or bypasses the technical measures taken by data producers or controllers. Therefore, if the defendant does not have such behavior (such as only using others' published data), the application of the "principle clause" may be considered for adjustment of such behavior.

4. Judgment of the Legitimacy of Data Competition Behaviors

In practice, the indicted behaviors in data competition disputes usually include data grabbing and data using. When judging whether the indicted behavior is legitimate, it should be considered from the type of

the data involved in the case and the specific performance of the indicted behavior.

4.1 Types of Data Involved in the Case

From the perspective of data types, network operators often distinguish the types of data in their platforms by means of "front-end data" and "public data", but there are no uniform opinions for the understanding and definition of data under such distinguishing mode, and from the technical perspective, there may be scope overlaps of such distinguishing mode or loose classification. Therefore, from the normative level, it is more meaningful to distinguish the concept of "public data" and "non-public data". Under this type of distinction, generally speaking, data for which the data controller has no access authority and can be viewed without any identity authentication or user login belongs to public data, and data for which the data controller can be viewed only by setting access authority through login rules or other technical measures should be non-public data.

4.2 Performance of the Indicted Behavior

For non-public data, its coefficient controller has taken certain technical measures to set access authority. In the absence of cooperation or authorization, the data user can only use technical means to destroy or bypass the access authority taken by the data controller, which is obviously improper. Because the act of grabbing itself is improper, it is also difficult to say whether the subsequent use of non-public data is proper.

The legitimacy of grabbing and using of public data shall be determined comprehensively based on the following specific circumstances.

4.2.1 Grabbing but not Using

For the public data in the platform of the data controller, based on the characteristics of data integration and interaction in the network environment, the platform operator shall, to a certain extent, tolerate the legal collection or use of the public data in the platform by others. Otherwise, it may hinder the application of data for public welfare research or other beneficial uses and is contrary to the spirit of interconnection of the Internet. Therefore, the legitimacy of grabbing of public data mainly depends on whether the grabbing by the defendant complies with legal obligations and industry rules. In the network environment, if a data user obtains relevant data through legal and proper means, such as manual record compilation or automatic grabbing of relevant data by web crawler technology that complies with general technical rules, the grabbing of data shall be deemed proper.

However, not all behaviors of grabbing public data but not using them are justifiable. For example, in order to be displayed in search engines, network operators generally will open the data on their webpages to be grabbed by search engine service providers and other web crawlers. However, in order to prevent negative impacts such as the effect of market substitution, increased burden on servers and frustration of performance of the user agreement caused by data grabbing behavior to their products or services, some network operators will refuse part or all of the crawling of their data by setting up the Robots Agreement on their webpages. At this time, although the network operator acting as the data controller sets certain obstacles to access to the data under its control, from the perspective of data

classification, the Robots Agreement is to some extent a "gentlemen's agreement" due to its lack of normative effect. Therefore, this part of data that is not allowed to be accessed is also public data that is directly accessed upon opening the operator's webpage and no special access rules are set up for it. In this case, the Robots Agreement set up on the webpage by network operators is usually considered as reasonable. Therefore, if a third party grabs a large amount of such public data without complying with the restrictions set up in the Robots Agreement, even if it does not use such data, it may still be improper because the data grabbing affects the business interests of others such as data security.

4.2.2 Grabbing for Direct Use or Use after Simple Processing

For legally obtained public data, whether the grabbing and use is proper, a court may determine whether the act in question hinders or destroys the normal operation of others' platform from the perspectives of the data controller's performance of the user agreement, impact on the exclusive data rights and interests, investment in and returns of data security, completeness of the data presentation rules, whether the act in question constitutes a substantial substitute for the original platform, and the impact on the economic benefits that the original platform can generate based on the data rights and interests, so as to judge whether the act in question is proper. If grabbing a large amount of data competition resources are generated by data controllers through long-term operation and accumulation, and the corresponding data are directly copied and used, it shall be improper that the defendant has used the data beyond the necessary limit and reasonable scope even though the grabbed data is public data.

In practice, it is rare to obtain public data for direct use; on the contrary, after obtaining the public data of others, a data user will, based on the type and characteristics of the service provided by itself, screen and integrate the data obtained from the data controller to a certain extent, and then reveal and use such data on its platform. For example, the vertical search used by search engine service providers refers to the search conducted within a specific scope for an industry and after mining and integration, the search results are fed back to users in a certain form. From the perspective of technical characteristics and the nature of behavior, such behavior is also to present to users the data originated from the control of the data controllers, but there is not much difference from grabbing and direct use when no in-depth extraction has been carried out. Therefore, such behavior of grabbing public data for appropriate processing and use shall still be limited within a reasonable scope, and follow the principle of "necessary and minimum", so as to avoid homogeneity and substitution for the data controllers.

4.2.3 After Grabbing, Go through Secondary Processing and Become New Data Products for Use

Development and market application of data products is one of the business models in the current internet industry. For example, internet operators usually predict users' preference by analyzing users' consumption data, so as to improve their products and services. If a data user grabs public data through a legal channel, and deeply filters, cleans, edits, and integrates the grabbed data to form a new data product, then, although the relevant original data originate from the data controllers, the final data product is formed through the data users' creative input, and has departed from the original data form,

and is legitimate in both the means of grabbing and the way of use, which also helps to improve consumers' user experience, so it shall not be deemed as unfair competition. For example, in the case of HiQ v. LinkedIn, HiQ, as a data analysis company, used a web crawler to obtain public profile information of LinkedIn users, and processed and analyzed the data to form data products such as personalized career advice for sale. The US Courts held that the value and utility of a large amount of public information depend on the finding, collection, arrangement and analysis of such data, and that HiQ's business model and position were preferable in the public interest. At the same time, taking into account the impact of LinkedIn's restriction of crawling on its competitors' competitive advantage in the data analysis market and the realization of the value of data, the decision to prohibit LinkedIn from adopting anti-crawling measures against HiQ was made.

5. Conclusion

When judging the legitimacy of data competition, technology, business models themselves, and competition implemented by new technology or based on new business models should also be distinguished.

Data competition is often associated with technological innovation. Admittedly, in the network competition environment, efficient and comprehensive acquisition of data will indeed stimulate technological innovation. However, the innovation of a technology does not necessarily mean that all the activities based on such innovative technology are legitimate. As in the unfair competition dispute between Beijing Weredream Chuangke Network Technology Co., Ltd. and Shanghai Foyo Culture & Entertainment Co., Ltd., the method of Feiyou App to obtain information on Weibo would certainly use a different data obtaining technology. However, the technology itself is only a carrier, and therefore the illegitimacy of the involved act of using such technology to destroy the technical measures on Weibo platform cannot be denied.

Therefore, when judging whether the indicted conduct is justifiable, although the factors of data producer, data controller and data user must be taken into full consideration, the indicted conduct itself is always the primary consideration when judging whether it is justifiable. The defendant may not be allowed to infringe upon the legitimate rights and interests of others on the ground that the technology adopted by the defendant belongs to innovative technology or the business model developed by the defendant is in line with the development of the times.

The current data rights and interests legislation is relatively backward, which makes the choice of data protection path difficult, and also contradicts the gradual highlighting of the value of data. The judiciary should act accordingly, provide corresponding protection for data under the existing legal framework in accordance with the law, timely respond to the data protection needs of network operators, and draw boundaries for data competition that has not been standardized at present, so as to regulate the data competition order in the relevant market.

References

Cheng. X. (2018). On Personal Data Rights in the Big Data Era. *Chinese Social Sciences*, *2018*(03), 102-122, 207-208.

Hu, 73., & Min, Z. (2016). *No. 242*.

Jing 0108 Min Chu No. 24510. (2017).

Zhang, Q. K. (2015). Logical Analysis of the Application of the General Clause of the Anti-unfair Competition Law—A Case Example Concerning New Internet Unfair Competition. *Intellectual Property*, *2015*(03), 30-36.

ZHAO, W. H. (2010). *On the Improvement of Intellectual Property Protection System for Data Bases*. Beijing: China University of Political Science and Law, 2010.

Zhou, H. W. (2019). Exploring Intellectual Property Protection of Non-original Databases. *Henan Science and Technology*, *2019*(06), 32-35