ISSN: 2688-8653

Thoughts on Anti-monopoly Law of Data Privacy Protection

Jingyun Wo*

School of Anhui University of Finance and Economics, Anhui 233000, China

Abstract

In the era of digital economy, data has important commercial value, and the privacy behind it has attracted the attention of antitrust law. As an important non price factor, data privacy is an important embodiment of consumers' interests, and can be used as an important factor for enterprises to enhance market power. From the perspective of competition law, there is a certain theoretical basis for the protection of data privacy into the consideration of antitrust law. When considering the Anti-monopoly law, we should use the traditional means of Anti-monopoly law, such as business concentration, abuse of market dominant position, etc. in addition, we also need to pay attention to the attention of consumers to data privacy.

Keywords

Data Privacy; Non Price Factors; Concentration of Business Operators; Abuse of Market Ascendancy.

1. Raising Questions

The development of Internet technology has brought earth shaking changes to people's lives. On the one hand, the development of digital technology has brought convenience to life and improved living standards. On the other hand, in the era of digital economy, the data security problems brought by digital technology in the operation process are also worth pondering.

The development of digital economy largely stems from the integration of data and cloud computing technology, both of which are indispensable. Data, like oil, is a valuable resource in the 21st century. It can be said that in this era, whoever has the data will seize the opportunity. At present, digital platforms that are closely related to life, such as social networking, shopping and search engines, monitor the needs of consumers by collecting, processing and analyzing the user information obtained, supplemented by algorithm means, carry out personalized positioning, push the advertisements predicted by the platform that meet the needs of consumers, and implement differential pricing, that is, the well-known behavior of "killing ripe big data", So as to achieve the best effect of data use. After such a process, the digital platform can realize the data it has and continuously gather more data, so as to form its own competitive advantage. In order to consolidate its own advantages, the platform will build high industry barriers by refusing data opening and mergers and acquisitions of small enterprises, hinder the entry of competitors and hinder the normal competition order. However, many of these data used by the platform as a means of competition are composed of users' personal information, such as identity information, family situation, property status and so on. This information does not only belong to the platform. When competing with each other, the platform takes the data information as a chip, which also infringes on the user's personal privacy to a certain extent. Therefore, data involving personal information can not only bring economic benefits to platform enterprises and help form competitive advantages, but also its personal information attributes. Therefore, the infringement of users' privacy by large digital platform enterprises through their data advantages and market dominant position not only violates the market competition order, but also infringes on users' right to privacy, resulting in the intersection of

ISSN: 2688-8653

antitrust law and privacy protection, which is quite controversial in the theoretical and practical circles.

There are different views on whether the protection of data privacy is regulated by antitrust law.These different views mainly focus on the legislative purpose of two fields and the specific application of Anti-monopoly law. Supporters believe that the Anti-monopoly law and the personal information protection system have a common goal in the protection of consumers' interests. First of all, from the perspective of the subject, the Anti-monopoly law believes that competition can promote the interests of consumers, while for the personal information protection system, the subject of its protection is the parties to personal information, which is actually consumers. Secondly, from the perspective of regulation, the Anti-monopoly law is mainly to control the market force and reduce its impairment to the interests of consumers. Similarly, the personal information protection system is to prevent information subjects from being infringed when sharing data. Therefore, whether from the perspective of subject or implementation content, antitrust law and personal information protection law are consistent in data privacy protection and can be implemented together. [1] Opponents believe that the legislative purposes of the two are different. The Anti-monopoly law tends to market competition order and economic efficiency, while the personal information system focuses on the protection of personal rights and interests. The Anti-monopoly law also has a fixed analysis framework. If personal information is included in it, the Anti-monopoly law will lose its professionalism, its framework boundary will be broken, and it is easy to become a bottom clause.

In Facebook's acquisition of WhatsApp, user information is one of the important factors in Facebook's decision to acquire. Both have a large number of users and highly overlap in business. Facebook obtains each other's user information through acquisition, and uses these data to expand its market influence and enhance its market position. This case shows that in similar data-driven mergers and acquisitions, it is necessary to evaluate the value of the data, that is, the market value contained in the data. In the actual platform merger, if we do not consider the protection of data privacy, we only evaluate the market influence and other factors of the platform. This way is to protect the overall interests of both platforms on the basis of losing the interests of some users. It seems to be more in line with the business philosophy of putting economic interests first among enterprises, but in fact, it has lost more valuable long-term interests.

2. Competition Law Value of Data Privacy Protection

There are also provisions on the definition of privacy in China's civil code, but the provisions are relatively broad and do not explain the extension of privacy clearly. In this regard, there is a fair conclusion: privacy is an inviolable personality interest, which is related to the control of information. [2]This statement is also recognized in the era of big data. Privacy often intersects with data and information and is expressed in the form of data. Operators also find the value of data privacy. By analyzing and processing data, they can obtain users' privacy, so as to better understand users' consumption preferences and provide users with more suitable products. However, in this process, the platform often ignores the protection of users' personal privacy, takes the collected data as its own, and takes some violations of personal privacy without users' consent or forced users' consent. Similarly, in data-driven enterprise M & A, the reason why some powerful enterprises choose to acquire some small enterprises with great strength is likely to be the personal data owned by small enterprises. Then after the two are concentrated, these consumer data are transferred to large enterprises as assets, and large enterprises extract their value by integrating these data. Therefore, with the development of the Internet, privacy has become an important contemporary proposition. From the

ISSN: 2688-8653

perspective of law, privacy protection has its value in competition law and needs to be regulated by Anti-monopoly law.

2.1. Data Privacy as a Non Price Factor

The biggest consensus on the relationship between antitrust and privacy protection may be that consumer privacy is an important dimension of non price competition. For a long time, many platforms claim that they provide "free" services, which will not cause economic losses to consumers, so they will not harm consumers. This statement has attracted the attention of antitrust law.

In the Microsoft antitrust case, they believed that users received the "free" software Internet explore browser in the form of Microsoft, which would not harm consumers. This approach seems reasonable, but it can not stand business-related review. There are many such cases. There are large Internet giants such as Facebook, Amazon and Google in foreign countries, and wechat and other platforms in China. In these business models, consumers do not receive "free things", but "pay" with their personal data. Therefore, antitrust can and should adapt to non monetary payment, otherwise important consumers may suffer from inaction. In fact, the platform business model often forces consumers to agree to privacy terms through its market position, and uses its dominant position to obtain more consumer data privacy. The director of the German antitrust bureau believes that Facebook occupies a dominant market position in the social field and should bear higher social responsibilities than other enterprises to maintain the normal operation of market order. Therefore, based on this dominant platform, users' acceptance of privacy terms is not objective and can not be used as the basis for users' disposal of data privacy. In the case of Facebook and what's app, the European Commission held that if the merged platform starts to require users to provide more personal data or start providing such data to third parties as a condition for providing them with "free" products, this can be regarded as raising prices or reducing product quality, and constitutes a violation of competition law. These seemingly free services are actually realized through the exchange of personal data. Different from traditional enterprises, Internet platform naturally has network effect, which means that "free" can also be realized. Obtain consumer data through "free", collect and sort out these data, depict the image of consumers, and then provide targeted services for consumers. In this way, consumers will habitually choose this platform, and the platform will continue to collect more data irrelevant to consumers' use of the platform, such as the opening position required by the photographing software, and the photo information required by the takeout platform. These behaviors have had an impact on consumers' privacy, and consumers often do not realize or have realized that they have to give up the protection of privacy because of "habitual choice". Whether the former or the latter, consumers are in a weak position in front of the platform.[2] The fact that consumers provide personal data in order to obtain the right to use the platform is a concrete embodiment of the abuse of market dominance by enterprises. On the surface, the setting of privacy terms of enterprises gives consumers the right to choose and respects the idea that consumers want to protect their privacy interests. In fact, it puts a yoke on consumers and gives enterprises a legitimate reason to collect data.

2.2. Data Privacy as a Consumer Benefit

A mature consumer market must be accompanied by the high-speed circulation of information, especially in this era of digital economy. This information is largely composed of personal information. Some of these personal information can be made public, while others are closely related to personal privacy. For individuals, this is enough to depict the privacy of their own image, and from the perspective of operators, this is the convenient condition for grabbing profits. From Article 14 of China's consumer protection law, we can see that China attaches great importance to privacy protection, that is, when consumers consume in the trading market,

ISSN: 2688-8653

their privacy information should be respected. If privacy is violated, it is a derogation from the interests of consumers.

When analyzing consumers' behavior towards data privacy, we have to consider the statement of "privacy paradox". This statement refers to the inconsistency between consumer awareness and behavior, that is, consumers pay great attention to data privacy, but in specific links, they will give priority to product quality over privacy protection and pay more attention to the product itself. [3]This phenomenon suggests that consumers may not pay much attention to privacy, but more attention to other interests. Therefore, we don't need to pay so much attention to the privacy of consumers, but should pay more attention to the possession of market share and the enhancement of product characteristics. In fact, this statement is not combined with the current situation of digital economy, which leads to such a deviation of consciousness.

Consumers are unable to make proper arrangements for their behavior, which is affected by other factors under the digital economy to a certain extent. Firstly, there is information asymmetry between consumers and operators. In the digital economy, platforms often launch "zero price" products or services to obtain users' personal data with temporary low profits. In the case of free products or services, users pay no price.In addition, for consumers, the loss caused by their shared data is uncertain and will not be reflected at the moment, but the products or services obtained can be realized immediately. Based on this, not all consumers clearly understand the long-term significance of data privacy. Even if they do, they may over share data privacy due to their current "shortsightedness". At the same time, the privacy settings of Internet platforms are often vague. Privacy settings are the presentation form of privacy protection that consumers intuitively feel. At present, the privacy settings of various platforms are usually very lengthy. The opportunity cost for consumers to understand the specific content of privacy settings is huge. Moreover, some platforms with a dominant market position are often set up. If they do not agree with the privacy policy, they will not be able to use the platform normally. This practice makes the platform in an unequal relationship with consumers, and consumers have little space to choose by themselves.

2.3. Data Privacy as a Way to Enhance Market Power

Generally speaking, if an enterprise takes the protection level of data privacy as an important factor in enterprise development, it should be recognized by consumers. In practice, many platform enterprises and even other Internet enterprises with dominant market position take the infringement of user privacy as a means to enhance their market power. This is because the digital economy has network effect and locking effect, that is, the platform enriches product content by continuously collecting data, so as to gather a large number of users, and then analyze these users to improve product quality or service experience, so as to attract more users; The platform can also improve the accuracy of the algorithm through the obtained data, harvest more funds, and then optimize its technical level again. These two processes are a continuous circular process, linked, which is also the operation means of most platform enterprises. They use data to collect data and improve algorithms to achieve a high concentration of capital and form economies of scale. As a result, the power of large enterprises is becoming stronger and stronger, and its power can be transmitted to other similar or cross-border enterprises, and form a mandatory on consumers, including but not limited to compulsory consent to privacy policies, collection of user data and other behaviors. At this time, consumers have changed from enjoying the "zero price" service obtained by sharing data to losing their bargaining power. This unequal position will become more and more intense as Internet enterprises continue to collect data and expand their power. Therefore, from the perspective of competition law, the behavior of Internet enterprises to enhance market power through continuous data collection shows that the market will lose the original benign

ISSN: 2688-8653

competition, damage the interests of consumers, and is not conducive to the normal operation of market order.

3. Damage Analysis of Data Privacy under the Framework of Antitrust Law

Analyzing the damage of data privacy within the Anti-monopoly framework is generally inseparable from these three aspects, namely business concentration, abuse of market dominant position and monopoly agreement. However, there is no case involving the data privacy of monopoly agreement, so only the damage to data privacy in the first two aspects is discussed below.

3.1. Concentration of Business Operators

The problem of business concentration is often associated with the problem of data privacy. This is because under the digital economy, a large number of data-driven enterprises are involved in the collection and use of data. Once there is a merger between these enterprises, it is likely to reduce the level of consumer privacy. For example, in the case of Microsoft's acquisition of LinkedIn, Microsoft can pocket the rich user career information mastered by LinkedIn, so as to facilitate its more accurate delivery of data to users. Such mergers and acquisitions are guided by consumer data privacy. After the merger, we can obtain more consumer data and occupy more market share. In this way, enterprises will lose the power to protect data privacy by paying capital, and the choice space of consumers will become smaller and smaller due to such data concentration, which is not conducive to the protection of consumer data privacy and the virtuous circle of the market.

In the practice of extraterritorial law enforcement, data-driven business mergers are often reviewed by antitrust authorities, because it is very common for these enterprises to improve profits by impairing consumer privacy. For example, in the case of Facebook's acquisition of WhatsApp, the US Federal Trade Commission (FTC) actually approved this behavior, but added Facebook's obligation to perform, that is, it must promise not to compromise users' privacy. Similarly, in the case of Microsoft's acquisition of LinkedIn, the European Commission also proposed to consider privacy as an important non price factor. However, all law enforcement agencies should ultimately implement it in accordance with relevant laws. Therefore, even though many law enforcement agencies have understood the importance of data privacy to censorship, they are often helpless when it comes to assessing the non price factor of private data in practice.

3.2. Abuse of Market Ascendancy

The two magic weapons in the era of digital economy are data and algorithms. When enterprises with a large amount of data use algorithms to continue to improve data accuracy, such enterprises are likely to occupy an important position in the industry, that is, they have a dominant market position. When an enterprise is indeed an enterprise with a dominant market position and uses this dominant position to collect usage data, the infringement on the level of consumer data privacy protection will involve the abuse of a dominant market position.[4]

Generally speaking, Internet companies with a dominant market position usually gather a large amount of consumer data, and will also collect more data in various ways. If the enterprise has the actual or expected consequences of reducing consumer privacy in this process, it may constitute exploitative abuse. At this time, it needs to use the tools of Anti-monopoly law for reasonable regulation. When an enterprise's dominant market position is formed due to the continuous collection of user data, such behavior violates the data protection law. Taking Facebook as an example, when the German competition law enforcement agency punished it, it included privacy protection into the abuse of market dominance. This is also the first time that

ISSN: 2688-8653

the Anti-monopoly law enforcement agency has associated privacy protection with the abuse of market dominance in practice. The German antitrust regulator Federal Cartel Office (hereinafter referred to as FCO) pointed out that Facebook has a dominant position in the German social market because it occupies more than 90% of the market share. For users, they can only choose Facebook as a social means, and they can't decide how their data is processed. Facebook itself does collect and use data without the user's knowledge. Thus, in 2019, FCO ruled that Facebook abused its dominant market position and restricted its illegal data phone behavior in Germany. After Facebook filed an appeal, the German Federal Court ruled in support of the FCO's allegations. [5] Facebook's use of its dominant position in the social industry to collect and use user data not only infringes on consumers' privacy and damages personal rights, but also hinders industry competition and increases industry barriers. Anti monopoly law should be applied to regulate this kind of behavior.

4. Antitrust Law Response to Data Privacy Protection

Data privacy is a new problem in the digital economy, but it will lead to the phenomenon of damage to consumers' interests and competition. The regulation of Anti-monopoly law has a theoretical and practical basis. In the era of digital economy, data has triggered these problems and brought people new thinking. Should we push through the old and bring forth the new to adapt to the development of the times? In fact, the law is stable and inclusive. The emergence of new things is unexpected. In order to maintain the authority of the law and carry the development of new things, we need to make appropriate adjustments to the original law so that it will not be invariable or too rigid. Most scholars also believe that digital economy is not enough to shake the basic principles of Anti-monopoly law, so we only need to make appropriate modifications within the framework of traditional Anti-monopoly law. Based on this, this paper will think about the problem of data privacy from the perspective of antitrust law, and put forward some suggestions.

4.1. Consumers' Attention to Data Privacy

A full understanding of consumers' attention to data privacy plays an important role in how to protect and how to protect data privacy. When analyzing the importance of data privacy in the consumer market, the attitude of consumers is very important, because consumers are opposite and have strong subjective consciousness. If consumers pay great attention to their own data privacy and operators will consider this factor in market competition, it is more meaningful to adopt Anti-monopoly law regulation. Nowadays, consumers pay more and more attention to data privacy,[6] However, from the "privacy paradox" mentioned above, whether we pay attention to it is affected by many factors, such as information asymmetry and the setting of privacy policy. And the development of digital economy is changing rapidly, and operators are constantly changing their business means. Consumers' own judgment is not enough to support their attention to data privacy. They are often disturbed by various external factors, so that they can't judge whether they really pay attention to data privacy and how to fully protect data privacy. Therefore, for the protection of data privacy, from the perspective of consumers, we should consider individual cases and make judgments after fully understanding the characteristics of consumers.

Both information asymmetry and privacy settings reflect the corresponding relationship between consumers and operators. To analyze consumers' attention to data privacy, we have to evaluate the impact of operators' behavior on consumers in the digital economy. Firstly, digital economy has network effect and lock-in effect. Take the instant messaging provided by wechat as an example. After wechat was launched, it met the social needs of consumers, so it gathered a large number of consumers, and gradually occupied the social market with the increasing volume. In addition, other software such as games, e-mail and other life software can

ISSN: 2688-8653

be applied to wechat login. Therefore, wechat realizes binding relationship not only in the social module, but also in other modules. At this time, consumers can no longer choose other social software, and wechat has realized the locking effect. Secondly, due to information asymmetry, consumers cannot understand the extent to which operators collect data privacy and the infringement of this collection means on consumers. The setting of privacy clauses of operators often blurs the key points. Some consumers who do not have professional knowledge cannot capture the meaning, and some consumers ignore the privacy clauses because of time cost or more emphasis on product quality. In addition, most operators force consumers to agree to the terms by not agreeing to the privacy terms and not being able to enter the software. At this time, the "consent" of consumers is based on unequal relations and cannot be regarded as the real consent of consumers to the privacy terms. Therefore, consumers and operators are in an unequal relationship, and the decisions made by consumers based on this relationship can not represent the true attitude of consumers. In this case, we can't judge consumers' attention to data privacy blindly according to consumers' consent or disapproval of privacy terms, but we should analyze the specific situation and deeply explore the essence of this situation, so as to make a correct judgment on consumers' behavior.

4.2. Consideration of Data Privacy Interests in Business Concentration

Business concentration often infringes on consumers' data privacy. Therefore, in the merger and acquisition of data-driven enterprises, data privacy should be reviewed, and data privacy should be considered in the review. The impact of data privacy on the interests of consumers should also be taken into account.

First of all, for the data privacy occupied by business operators, the amount of data, data analysis ability, data collection and processing ability should be considered together. Specifically, the more users an operator has, it generally means that it covers a large amount of user data. Moreover, whether the data owned by operators can be carried and copied is also an important factor for enterprises to face privacy risks in merger. In addition, after business concentration, review whether the merged enterprise has a larger amount of data and whether its data analysis and processing capacity has been enhanced.

Secondly, the impact of business concentration on the interests of consumers. The interests of consumers are closely related to the protection level of data privacy. The interests of consumers are also the visual embodiment of whether the concentration of business operators complies with the provisions of the Anti-monopoly law. During the review, the expected damage to the interests of consumers should be predicted according to the business conditions and business habits of the operators. We can also learn from the practice of FTC on Facebook and require the operators to make a commitment to the protection of consumer privacy.

4.3. Consideration of Data Privacy Interests of Abusing Market Dominance

Due to the particularity of the data economy platform, operators will pay more attention to the commercial value brought by data, thus ignoring the user privacy protection behind data. Especially the operators who occupy the dominant market position have made huge profits by infringing on the interests of consumers. It is impossible to regulate them through the market mechanism, so it is necessary to regulate them through the Anti-monopoly law.

As mentioned above, the violation of consumer data privacy by operators with a dominant market position may constitute exploitative abuse. In this case, the identification of this behavior should not focus on subtle considerations, but should be analyzed in combination with the overall interests, not only to protect data privacy, but also to ensure that it does not destroy the original market vitality and maintain the normal market competition order. Therefore, in law enforcement, flexible application of law can be considered: different amount of law enforcement intensity can be given according to the openness of the market. Specifically, in a

ISSN: 2688-8653

highly concentrated market, enterprises with a dominant market position carry out a large amount of data collection and data analysis to undermine the market order. In the face of such behavior of significantly enhancing their own market power and reducing competition, law enforcement agencies should actively enforce the law; In a more flexible market, dominant enterprises do not occupy a high market share, and enterprises can maintain normal competition, then some less privacy derogation behaviors at this time can be ignored. [7] In this way, we can make proper arrangements for the interests of consumers without destroying the original market mechanism.

Acknowledgments

This work is supported by the Postgraduate Research and Innovation Fund Project of Anhui University of Finance and Economics, Project Number: ACYC2021086.

References

[1] Louise O'Callaghan: How to Incorporate Data Protection, as a Non-Economic Objective, into EU Competition Analysis, The Intersection Between Data Protection and Competition Law, Vol. 109 (2018) No.21,p.111.

[2] Ming Xu:Privacy crisis in the era of big data and its response to tort law，China Legal Science, (2017) No.1, p.130-149.

[3] Yuting Wang:Consideration of antitrust law on privacy and data protection, Journal of Northeast University (Social Science Edition),Vol.24(2022)No.1,p.104-111.

[4] Wei Han: Privacy protection and abuse of dominance in digital economy, Journal of Graduate School of Chinese Academy of Social Sciences,(2020)No.1,p.37-45.

[5] https://www.sohu.com/a/403946022_161795?_f=index_pagefocus_1&_trans_=000013_sjcl_zsmh.

[6] https://oversea.huanqiu.com/article/9CaKrnK6v8b?w=280.

[7] Jin Sun,Zhaozong Wan: antitrust regulation of abuse of market dominance and infringe.