Protection of Trade Secrets in the Context of Big Data: Dilemma and Improvement Path

Yi-Lin Xia[1], Zhi-De Zhou[2*]

[1]*Law School/Intellectual Property School of Guilin University of Electronic Technology*
[2]*Intellectual Property Research Institute of Xiamen University*
[*]*Corresponding author. Email: 854167177@qq.com*

ABSTRACT
Under the background of big data, trade secrets have also appeared in a new form of business, and data and trade secrets have crossed and overlapped. In the context of big data, trade secrets in the new form are facing a complex living environment, and cannot be effectively protected under the current law. Under the background of big data, the criteria for identifying trade secrets are not clear, there is a conflict between trade secret protection and personal information protection, and there are loopholes in the provisions of the burden of proof, so as to analyze the protection dilemma and improve the protection path.

Keywords: *Big data, Trade secret protection, Intellectual property, Cloud services.*

1.INTRODUCTION

Big data satisfies three major factors inherent to data, namely data structure, data manipulation, and integrity constraints. It can process information assets at high speed, with diverse data sources, low value density, high authenticity and high growth.[1] The processing of data is no longer limited to the traditional sampling analysis, and the use of high-tech means for timely and effective target information analysis of big data is more conducive to the development characteristics of the high-speed economic era. The sources of big data include people, computer systems, and digital equipment collection.[2]Based on the characteristics of big data, its collection, storage, operation and analysis will require a large amount of human and material resources, and even need to be constantly updated with the development of high-tech means, such as cloud storage, cloud computing, etc. to meet its collection, storage, operation and analysis conditions. For the definition of the connotation of trade secrets, it contains three elements, namely, “not known to the public”, “with commercial value”, “to take appropriate confidentiality measures”.The formation process and output results of big data are secret, because it can have economic value as a competitive advantage of market institutions, and it has confidential management for their use and protection. Therefore, big data and business secrets overlap under certain conditions.[3]

In the era of big data, the value of data is becoming increasingly prominent, which can bring economic benefits and bring commercial value, which meets one of the elements of trade secrets, “has commercial value”. As a strategic weapon for the development of competition between the same industry, the value of trade secrets is also self-evident. If the enterprise develops and utilizes big data to make it meet all the requirements of trade secrets, then the data and trade secrets have cross-overlapped and have the characteristics of synergy. The effective use of data in the era of big data needs to solve the problems of data collection, storage, operation, and analysis, so trade secrets in the form of data also face these problems.Therefore, a series of protection issues derived from big data will collide with the traditional trade secret protection system, and the protection of trade secrets in the era of big data will face new difficulties and challenges.How to solve the problem of trade secret infringement and protection in this series of processes needs to be based on the complex environment in the era of big data, and take targeted measures to solve it according to the synergistic characteristics of big data and trade secrets.

2. THE DILEMMA OF TRADE SECRET PROTECTION IN THE ERA OF BIG DATA

Trade secrets have the meaning given to them by traditional law, but in the context of big data, how to

make the protection of trade secrets in line with the characteristics of the times, it is necessary to improve the legislation and the use of judicial interpretation of the new interpretation. Big data era, the data to trade secret protection, must be based on the synergy of the two. However, the existing law has some loopholes that lead to the data become trade secrets for the protection of the identification standard is not clear, trade secret rights and other rights between the protection of conflict, high-tech infringement means caused by the difficulty of proof, need to be analyzed one by one to solve the problem.

2.1. The standard is not clear

Article 21 of the Provisions on the Protection of Trade Secrets stipulates the burden of proof on the right holder: the right holder shall provide the business information it possesses that meets the statutory requirements for trade secrets. However, in the era of big data, the interpretation of the connotation of trade secrets is not clear, which brings difficulties to the proof of the right holder and the court's judgment.

2.1.1. Secret angle

The criteria for determining confidentiality are stipulated in the law, that is, "not known to the public".Items (1), (2) and (4) of Article 6 of the Provisions on the Protection of Trade Secrets believe that information that can be obtained from public channels does not constitute "not known to the public", but based on the unique perspective of big data background, it cannot be generally determined.

In the context of big data, there is a huge amount of data, and people's access to information is more convenient and diverse. People can get the information they want through search engines. So whether the information obtained from this public channel can become a trade secret is worth exploring. Under the condition of satisfying value and confidentiality, whether information obtained from public channels can be used as a trade secret needs to be discussed on a case-by-case basis.If the information obtained by the enterprise from the public channel goes through the screening process of "collection, storage, operation, and analysis", the public has no way to know it, and it should be deemed to meet the conditions of confidentiality.For the information obtained by the independent operation of the enterprise, whether it is further processed or not, it satisfies the condition that it is not known to the public, and may become a trade secret and be protected. If the information obtained directly by the enterprise from public sources is considered to be a trade secret, it will not satisfy the "unknown to the public" characteristic.

2.1.2. Value perspective

The criteria for determining value are based on the current legal provisions, that is, "have commercial value". Value encompasses the essence of utility, and as long as the relevant data meets the practicality characteristics, it will generate value, whether this value is obvious or potential for further mining. Value brings commercial benefits, which is very beneficial to the development of enterprises, which is the ultimate reason why trade secrets can be used as the object of intellectual property protection. Excavating the deep connotation of value, it is found that it has the following characteristics: First, value does not have durability.[4] The trade secret itself is not permanent, and it will no longer have the requirements of a trade secret for various reasons, such as accidental disclosure of information known to the public, so its value will be lost with disclosure. Second, value is not inevitable. The conception of the value of trade secrets requires a cumulative process, which requires a large amount of cost investment to maintain information. Therefore, the formation of value is not inevitable.Third, the value of trade secrets is not necessarily a state of completion. With the continuous maintenance and accumulation of enterprises and the updating and development of the times, the value of trade secrets is constantly changing. This change can be an improvement over the trade secret itself or an improvement on the non-trade secret.

2.1.3. Confidentiality perspective

The current law does not explain too much about the criteria for determining confidentiality. Only in the "protection of trade secrets" draft of the eighth article provides the corresponding confidentiality measures, which (a) (c) (d) provides for the confidential information set level of confidentiality, encryption, locking, decompiling and other preventive measures, the confidential information using passwords, codes, although these provisions show that our country's laws seek to protect trade secrets more perfect, but in the unique context of big data, still slightly inadequate In the context of big data, it is still inadequate. In the era of big data, data storage and processing will be used to the cloud platform, and there is no requirement for the degree of confidentiality when it comes to cloud storage. Confidentiality measures are designed to meet a state of exclusive possession of trade secrets by the possessor of trade secrets, and the confidentiality measures of trade secrets in the context of big data should be based on the ability to meet such a state of exclusive possession. Although the trade secret right holder can not require excessively harsh confidentiality measures, but still need to clarify the level of confidentiality of the cloud storage platform.

2.2. Conflict between trade secrets and personal information protection

Personal information and trade secrets are both objects of legal protection in China, and the law has different provisions for the protection of both. Users actively provide personal data when registering on the platform and operators collect personal data in the process of users' use of products or services are both common ways for operators to obtain data.[5] If personal information becomes customer list information held by the enterprise, i.e., becomes a trade secret of the enterprise, there will be a conflict of protection problem. The first paragraph (2) of Article 1035 of the Civil Code provides for the principle of public handling of personal information, which to a certain extent conflicts with the confidentiality required by trade secrets. In addition, as an object of intellectual property protection with commercial value, trade secret can be licensed just like patent. However, this is in conflict with the provision of the second paragraph of Article 1038 of the Civil Code of "no natural person shall illegally provide his personal information to others without consent". In the case that the business secret holder licenses the business secret to others, it is likely that the information will not be processed so that it cannot identify a specific individual.

2.3. There are loopholes in the provisions of the burden of proof

At present, the law provides that the burden of proof is borne by the first paragraph of Article 64 of the Civil Procedure Law, and the principle of "contact plus similarity" is used in judicial practice, but there are still some unreasonable aspects. In the Internet era, most of the trade secrets and technical information are stored in the cloud server, in the form of data. This also makes the illegal access to trade secrets means to achieve an upgrade, and illegal elements through illegal means, with electronic equipment as a springboard, with a high degree of secrecy, invasion, theft of enterprise trade secrets, so as to profit from the situation, the infringer even need only a certain performance of networked computer equipment, the use of hacking technology to achieve the infringement of trade secrets, such circumstances, due to part In this case, due to some of the trade secret rights of the technical limitations, the relevant rights of the person is difficult to specify the process of trade secret infringement, for the specific time and means of infringement can not prove, is not conducive to protecting the interests of trade secret rights. For example, Sina Weibo claimed that Pulse had used technical means to obtain its user data from the microblogging platform, but was unable to provide evidence of what improper technical means Pulse used because of the hidden nature of the network. In addition, to prove that the right holder has taken reasonable confidentiality measures, it must disclose the confidentiality measures it has taken, which will involve the storage technology, management technology, encryption technology of big data, etc. In the era of big data, these technologies themselves are the guarantee of data information security, which is the guarantee of the competitive advantage of the enterprise, and disclosing them to competitors will have the risk of technical leakage.[6]

3.THE IMPROVEMENT PATH OF TRADE SECRET PROTECTION IN THE ERA OF BIG DATA

Trade secrets is the object of intellectual property protection, but China does not have a special trade secret protection law, the general use of "anti-unfair competition law" and other relevant provisions of the law to protect it, the current "trade secret protection regulations" is in the process of consultation, the use of trade secrets of intellectual property properties, reference to its similar characteristics of the patent system to improve the regulations, On the other hand, we should also combine the new dilemma facing the protection of trade secrets in the context of big data, the use of judicial interpretation to cover the protection dilemma under the new situation, and build a perfect legal protection system of trade secrets.

3.1. Clear identification criteria

Under the background of big data, if enterprises store data in the cloud and set up password protection, it is necessary to further clarify whether "reasonable confidentiality measures" are taken. Some scholars believe that the confidentiality of stored data should be evaluated according to the division of public and private clouds, and public clouds do not belong to taking reasonable confidentiality measures, while private clouds belong to taking reasonable confidentiality measures, the reason for this determination is that although public clouds have set passwords, they are controlled by data managers, while private clouds are different, Unlike private clouds, where the data owner has direct control. In fact, whether it is a public cloud or a private cloud does not affect the security measures taken for the data, and if a public cloud is adopted, the enterprise can sign a contract with the service provider to agree on the security measures to be taken and the confidentiality clause. Therefore, it should be considered that both public and private clouds belong to take "reasonable confidentiality measures", but the premise is that the security of the cloud should reach a certain degree, and the cloud service provider's cloud technology and management level reach a certain level, which should be written into the contract signed between the enterprise and the cloud service provider.

3.2. Conflict of rights resolution

The data rights enjoyed by the subject of personal information, such as the right to be forgotten and the right to be carried, should be clarified. In addition, the priority of personal information protection should be clarified through judicial interpretation when an enterprise licenses its own trade secrets belonging to the category of personal information. The enterprise shall inform the subject of personal information of the corresponding information disclosed.However, the right to information enjoyed by an individual shall not infringe upon or improperly influence the business secret of the enterprise. Individuals maliciously violate the contract between the data controller and improperly exercise data rights such as the right to be forgotten and the right to be carried, which will seriously affect the normal production and operation activities of the data controller. At this time, the relevant individual rights can be restricted by means of proviso.[7]

3.3. Allocation of the burden of proof

Although enterprises are dissatisfied with some of the terms and conditions and try to negotiate with the cloud service provider, they often have little success because the cloud service provider is in a strong position. In the enterprise's trade secrets are infringed by some high-tech technology infringement after the difficult problem of proof. On the one hand, the trade secret is infringed because the storage technology provided by the cloud service provider is not safe enough, on the other hand, the cloud service provider is in a strong position in the contract with the enterprise caused by the substantial unfairness, in view of the reciprocity of rights and obligations in civil law, the cloud service provider can be legally obliged to help the enterprise to prove, if the evidence is unfavorable to bear certain adverse consequences.

4. CONCLUSION

As an innovative digital intangible asset, it is particularly important to maintain the security and confidentiality of trade secret data in the Internet environment. At present, the business secret protection of enterprises is facing a complicated environment. On the basis of clarifying the relationship between big data and trade secrets, it is necessary to find out the synergistic characteristics and protection dilemma of the two. On this basis, the legitimate rights and interests of the right holder of trade secrets should be safeguarded. The vitality of continuous research and development and innovation of enterprises should be stimulated. The healthy development of socialist market economy should be promoted.

ACKNOWLEDGMENTS

Guilin University of Electronic Science and Technology of China internet plus Intellectual Property Protection Research Think Tank (Guidian Xue [2019] No.3).

REFERENCES

[1] Zhu, Yang-Yong, and Eddie Xiong, Is big data data,technology, or application, in Big Data, 2015,pp.71-81.

[2] Andrea DeMauro,Marco Greco,Michele Grimaldi,Aformal definition of Big Data based on its essential features, Library Review, Vol.65,2016,pp. 129-130. DOI：10.1108/LR-06-2015-0061.

[3] Yu F L, Zhang G.Research on the protection path of big data intellectual property law -- from the perspective of trade secrets,Guangxi Social Sciences,2020,pp.102. DOI：10.3969/j.issn.1004-6917.

[4] Zheng Xuanyu,Zhou Yetian. A Preliminary Study on Trade Secret Protection in the Big Data Environment: From the Perspective of the Fan List of Corporate Social Accounts, Wuling Academic Journal,Vol.42,2017,pp.54. DOI:10.16514/j.cnki.cn43-1506/c.2017.04.007.

[5] Zhu, Andy, Legal attributes and legal protection of commercial data in the context of big data, Zhejiang University, 2018.

[6] Yang Xiongwen, Huang Yuanhui, On the Protection of Trade Secrets of Big Data - Taking the Case of Sina Weibo v. Pulse Unfair Competition as a Perspective, in Journal of Chongqing Technology and Business University (Social Science Edition), 2019, pp: 138-145. DOI:10.3969/j.issn.1672-0598.2019.04.016.

[7] Yan Tian, The Conflict and Reconciliation between the Protection of Trade Secrets of Enterprise Derived Data and Personal Data Rights, in Journal of Hubei Second Normal College, 2019,pp.36-40.