Advances in Economics, Business and Management Research, volume 215
Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)

Analyze the Protection of Personal Data in the Big Data Environment from the Perspective of the Enterprise

Yuhao Li[1, a, *, †], Xinzhu Yan[2, b, *, †]

[1]*Law Institute, Beijing Institute of Technology, Beijing, China*
[2]*Intellectual Property Institute, Dalian University of Technology, Dalian, China*
[*]*Corresponding author. Email: [a]1120190185mail.bit.edu.cn, [b]zora@mail.dlut.edu.cn*
[†]*These authors contributed equally.*

ABSTRACT
In the era of big data, with the advancement of information technology and the popularization of mobile intelligent terminals, the amount of data generated and captured by human society has exploded. This article studies the current situation of personal privacy and other data leakage in China and its cause analysis, as well as improvement measures. For a long time, the extent of China's personal privacy and other data leakage has caused many controversies and thoughts. Massive data and information resources have become an important driving force that leads the transformation of human production and lifestyle and promotes the progress of the times. At the same time, the virtuality and openness of the Internet have also weakened the control of personal information of citizens, and the risk of personal information leakage has continued to increase. However, in view of the current reality that there are multiple factors affecting the personal information security of Internet users in my country including the high incidence of infringements, and the greater degree of harm, it is almost impossible to rely on a single subject or a single measure to control information leakage. Behind these problems, this article expounds the status quo from three aspects including enterprises, governments, and third-party platforms, and analyzes the root causes and other direct causes. For these reasons, this article proposes two measures to increase the supervision of enterprises and increase the punishment of illegal acts such as data intrusion, so that the security of personal information in our country can be guaranteed.

Keywords: *component; data protection; data leakage; enterprise*

1. INTRODUCTION

Big data is ushering in a major change of the times, and it is changing people's lives, work, and thinking [1]. In response to data leakage in China and the world, some scholars believe that in the era of big data, information has become an important strategic resource to promote the development of the national economy, so data has become a new field for countries to play [2] and increasingly, loads of companies wanted to compete for the "oil" of the new era [3]. As for the reasons for the current situation of information leakage in China, many scholars explain that new Internet technologies and new applications are emerging in an endless stream, cyberspace has become more open, and the flow of information and the frequency of use have accelerated, which has improved the efficiency of information resource utilization, but at the same time it has weakened citizens' personal information security control capabilities [4]. Indeed, in cyberspace, a large amount of personal information is stolen, sold and used maliciously, and information leakage has become an important factor hindering the healthy development of the Internet. Therefore, how to establish a balanced state of order between the protection of citizens' personal information security and the open sharing of Internet resources has become an important topic in the current advancement of my country's informatization process.

2. THE STATUS QUO OF INFORMATION LEAKAGE IN CHINA

In the big data environment, the privacy protection of personal data applications is a complex social issue that not only involves ethics, law, industry, technology, and many other fields, but also involves a large number

of individuals, groups, companies, and institutions [5]. At present, personal data collection, processing, and transaction activities are unprecedentedly active, and various innovations are emerging one after another [6], resulting in an increased risk of personal data privacy leakage. On the "3·15" Consumer Rights Day, a large financial institution was exposed to leaking customer information; insurance companies received several complaints from customers that their insurance information was obtained by other insurance companies every day; telephone frauds often worked, and the cause was nothing more than the user's detailed information was resold to illegal persons [7]. In recent years, personal data privacy leaks that have frequently erupted have caused different types and degrees of damage to individuals, while also shaking the credit system of the Internet and the entire society. Especially in 2020, the global new crown epidemic broke out. In this environment, a large number of new Internet products and services emerged as the times require, while helping to prevent and control the epidemic, it also further promoted the digital transformation of society. At the same time, security cyber threats such as security breaches, data leaks, and cyber fraud have become increasingly prominent [8]. It is no exaggeration to say that the current domestic and foreign data breaches are 'rushing to make headlines' [9]. It can be said that the frequent occurrence of network security incidents such as data leaks has become an unavoidable problem for any unit or individual that uses computers and the Internet. In the face of the current serious situation, the following will analyze it from other relevant parties except the individual himself.

2.1 Enterprise

As far as the current legislative direction is concerned, enterprises are the first responsible persons in data breaches. Enterprise data leakage mainly includes two types: negligent leakage and malicious leakage. Negligence disclosure mainly refers to the situation where the operating unit and its staff inadvertently disclose customer information in the business process of collecting, using and storing customer information, but due to weak information security awareness, customer information is lost. It mainly includes the following three types of situations: (1) Information leakage can occur during the collection process. The operating unit is not very purposeful in the process of collecting customer information. It collects personal information in general, and does not properly handle information that is not related to the business, resulting in leakage of customer information. (2) Information leakage can also occur during use. In the process of information use, the operating unit ignored the protection of customer information, leading to the abuse and leakage of customer information. (3) Information leakage may also occur during data storage. The operating unit loses the storage device during the information storage process or the system information is copied during the system maintenance process, which leads to the outflow of customer information. Malicious disclosure means that customer information collected by a data and information operation unit is maliciously trafficked to middlemen by insiders in order to obtain huge profits. This illegal act of maliciously leaking customer information has a very bad social impact on personal information security and industry development. DiDi Global Inc., as a rapidly developing emerging enterprise, is a typical example. On June 29,2021, DiDi Global Inc. travel app quickly updated a version of its privacy agreement that would take effect on July 7. DiDi Global Inc. clearly wrote, "your personal information we will collect will be stored and used in mainland China". The users need to agree the application to collect their personal information (including name, cell phone number, ID number, facial recognition feature, occupation information, audio and video recording, travel information, call recording, setting information, IP address, even mobile phone recharge record, integral store exchange record). Article 6 of the *Personal Information Protection Law*, which came into force on November 1, 2021, clearly stipulates "The processing of personal information shall have a clear and reasonable purpose, be directly related to the processing purpose, and adopt a method that has the least impact on personal rights and interests. The collection of personal information shall be limited to the minimum scope to achieve the processing purpose, and personal information shall not be excessively collected." However, compared with other taxi software on the market, DiDi Global Inc. has seriously exceeded the scope of personal information collection, and the protection of users' privacy is very insufficient.

More seriously, DiDi Global Inc. was pointed out that in order for enterprises to successfully list in the United States, it took the initiative to disclose domestic data to the United States. Some media predict that as an enterprise that has mastered a large amount of sensitive citizen personal data, DiDi Global Inc.'s data leakage will cause irreparable losses to the country.

2.2 Government

The government is the watchdog in the data breach. In the face of this situation, government departments have the following shortcomings: (1) The government supervision measures are relatively lagging. The main government departments currently responsible for network supervision include the industrial information industry department, the industrial and commercial department, the public security department, and the security department. Government departments' regulatory measures for network information security include market access permits, network real-name

registration, technical supervision, and subsequent accountability. However, compared with traditional illegal acts, online infringement has the characteristics of strong concealment, low cost of illegality, and large profit margin. In addition, online infringement generally involves a large number of people, a wide coverage area, complex damage assessment, and difficulty in investigating and obtaining evidence. This makes the government's existing regulatory measures often inadequate in the face of online infringements, and it is difficult to implement regulatory responsibilities. Criminals are taking advantage of the lack of government supervision to steal and sell personal information, and even use the data they possess to carry out criminal activities. (2) The government's self-regulatory system needs to be improved. Due to the lack of a standard system for the use of citizens' personal information within the government, a small number of government personnel have been tempted by interests to sell a large amount of private information about citizens to commercial institutions through illegal channels. This kind of abominable behavior of "supervising and stealing" by supervisors has turned the government into a source of information leakage, which not only brings bad social impacts, but also makes cyberspace information infringements more widespread.

2.3 Third parties

At the same time, some network hackers can still infiltrate some websites or personal terminals through techniques such as decoding attacks, code implants, and remote file containing vulnerability attacks to gain some or all control rights, and then copy the website’s internal database information and personal terminal private information. Therefore, technological intrusion is also one of the main forms of threats to network information security. Facebook, which is the world's leading photo sharing site and the world's largest social app, is a good example of showing that the data security of enterprises is always challenged. In 2018, Facebook was exposed to large-scale user information disclosure. Cambridge analysis company in the UK collected the privacy information of up to 87 million Facebook users without permission to analyze the user's behavior mode, personality characteristics, value orientation and growth experience, so as to push campaign advertisements for specific users. In 2019, Facebook was exposed that there was a server without password protection, resulting in the disclosure of 419 million user information, including the user's Facebook ID and the phone number associated with their account. In April 2021, it was revealed that Facebook was invaded by hackers, and 533 million users' personal data were exposed in three days, involving 106 countries and regions. The leaked information included users' account name, location, birthday and e-mail address on Facebook, which was very detailed. In October 2021, some media reported that more than 1.5 billion Facebook users' data were sold on the hacker forum.

People believe that Facebook's poor performance in security protection not only infringes upon the legitimate rights of individuals, but also has a negative impact on national democracy, At the same time, it can be seen from a large number of data leakage events of Facebook for several consecutive years that although Facebook continues to take measures to improve the security of applications, the problem of data leakage cannot be well solved, which directly reflects the challenge brought by the problem of data security to enterprises in today's era. It is worth noting that third parties other than hackers also have the risk of data leakage, but China does not currently have direct punitive measures. In recent years, WeChat Mini Programs (hereinafter referred to as "Mini Programs") have developed rapidly, but they have also exposed more prominent security risks, especially the risk of leakage of users' personal information. CNCERT had conducted security tests on the mini programs issued by 50 domestic banks from five dimensions including program code security, service interaction security, local data security, network transmission security, and security vulnerabilities. The results showed that there are 8 security risks in an average mini program. Over 90% of the mini-programs did not take protective measures when the program source code exposed key information and entered sensitive information; over 80% did not provide a personal information collection agreement; personal information was stored locally and during network transmission More than 60% have not been encrypted; a small number of small programs have serious risks of ultra vires. Therefore, at this point, the legislation needs to be stepped up and improved [8].

3. ANALYSIS ON THE REASONS FOR PERSONAL INFORMATION LEAKAGE

3.1 Root Cause

According to Baker's "risk society theory" [10], in the context of global development, global risks caused by human practice dominate the stage of social development. In such a society, various global risks have an impact on the survival and development of human beings. The grim situation of personal information leakage is actually due to the inevitable dilemma of the information age, which is a result of human practice, not a system defect.

From the status quo of enterprises, governments, and third-party platforms mentioned above, it can be seen that the deep-seated reason lies in the existence of deep-seated problems with the mechanism of corporate supervision and risk. Even the government can only play a supervisory role and the third party is an external threat,

not to mention an attack is a low probability event. As the main body of data transmission, storage, and utilization, enterprises have subjective responsibilities for data leakage. As a result, the focus of data supervision is to identify the behavior and legal responsibilities of enterprises, and the current penalties are unable to exert a good effect, especially the supervision concept is also a big problem. Therefore, in preventing data leakage, we should focus on the supervision and reform of enterprises.

3.2 Direct Causes

As for the analysis of the direct causes of superficial phenomena, combined with the diversity of data security subjects, it should be analyzed from multiple dimensions such as legal norms, operating unit responsibilities, and personal factors.

First of all, China's law started a little bit late for information protection. Fortunately, the existing Data Security Law and Cyber Security Law have already been implemented. However, unlike China's security protection obligations, which are based on national and industry standards and other necessary measures, European and American countries take concepts such as "reasonableness" and "appropriateness" [9] as the main evaluation criteria for security protection obligations. Adopting such a legislative model prevents the state from compulsory delimitation of a unified security model, and gives various enterprises and institutions sufficient space to formulate different network security strategies according to their respective business models. Perhaps it can be used for reference in our country's legislation.

Secondly, the governance of corporate data leakage has multiple dilemmas at the legal level: First at all, the responsibility for corporate data leakage is not clearly defined. The division of responsibilities between network service operators, data storage service providers, internal employees, and external third parties is not clear, and it is not clear how criminal, administrative, and civil liabilities are specifically applicable to laws and regulations. Besides, different countries have different legal systems regarding corporate data leakage, and the standards for defining corporate data leakage, responsibility assumptions, and extraterritorial application are not same [11]. In addition, he illegal costs and crime costs of leaking corporate data are relatively low, far lower than the corporate prevention costs, and the deterrence of relevant responsible entities is insufficient. Moreover, the long period for companies to deal with corporate data breaches through litigation or arbitration is not conducive to timely stop losses.

Finally, the status quo at the personal level is that Chinese citizens have a weak awareness of personal information security. Even if they have suffered from information leakage, most people choose to remain silent because they have not caused major losses. It is this victim's passive and conniving attitude that makes information leakage a normal phenomenon in cyberspace. At the same time, the network society itself is a virtual space based on modern information technology. Therefore, as a member of the network society, mastering the necessary information security technology is a prerequisite for ensuring self-security [4]. Individuals have become a vulnerable group in network information security due to their weak technical capabilities. Even if they find that network information is stolen, they cannot use technical means to stop network infringements in time, resulting in information leakage.

4. HOW TO PROMOTE DATA PROTECTION AT THE LEGAL LEVEL

To solve the problem of enterprise data leakage, we should first start from the source. And the source is the enterprise itself. Take Facebook as an example, we can draw a conclusion. The reason why data leakage occurs frequently is that on the one hand, the enterprise itself is poorly regulated, and on the other hand, the law does not pay enough attention to the behavior of data intrusion.

4.1 Supervision of enterprises

Requiring enterprises to strengthen the ability of data security protection through law is the first urgent problem to be solved. As mentioned above, the value of data in the big data era determines that once there is a lack of appropriate legal supervision, domestic and multinational companies will continue to expand the scope of their data and information collection in order to achieve business competition in the big data era. The most direct way to effectively avoid this situation is to strengthen the supervision and law enforcement of data violations and increase fines. Before 2021, China has no relevant laws to punish corporate data leakage. Although hackers who invade corporate data have been punished in some cases, enterprises have hardly been punished for data leakage. In China's latest laws, data leakage will be fined up to 10 million yuan, but obviously, such efforts are quite insufficient. For some large enterprises, such fines are not even enough to cause panic. China also needs to legally reflect the government's determination to further face up to the value of data, because in fact, it is difficult to set an upper limit on the importance of data and the value that data can output, and the ceiling of 10 million yuan is far lower than the punishment of many countries in the world. Compared with the mechanized setting of fines, China should explore how to match the number of fines with the value of leaked data.

Although China is accelerating legislation on data protection, such as the Data Security Law and the

Personal Information Protection Law. However, in addition to the one-off requirement that enterprises should establish a data security management system when processing data, there are no provisions to specifically require enterprises to strengthen their data security protection capacity, and there are no detailed punishment measures, which will lead some enterprises to collect data beyond their protection capacity, which is easy to be invaded and leaked to all over the world. Therefore, we should continue to refine the relevant enterprise data security management system on the basis of several newly promulgated laws, and limit the data that enterprises can collect to the scope that enterprises can absolutely protect. If there is no matching data protection capability, enterprises are not allowed to collect relevant data. And if the enterprise collects data beyond the specified limits, whether the data is leaked or not, the enterprise should be punished. In addition, relevant evaluation organizations should be established to regularly evaluate the data protection capacity of enterprises, and cancel their right to collect relevant data for unqualified enterprises.

4.2 Punishment for data intrusion

With the development of the Internet and the advent of the big data era, the value of personal information and data reached an unimaginable level in the past. The behavior of hackers has changed from curiosity and showing off technology to seeking benefits. But in many countries including China, the laws on hackers are still outdated.

Although we can find some cases online, such as a convicted hacker in Turkey received a 334-year sentence for data theft. But these cases likely obscure the fact that, in many countries, the crime of data theft most often is met with light or suspended sentences and monetary fines – not hard jail time. And these cases overlook the enormous number of small-scale leaks and data thefts happening on corporate networks all over the world. Many of these go unreported and the culprits never face criminal charges. This deserves the attention of all countries.

Similarly, taking China as an example, although the Internet technology and era are not what they used to be, China's legal basis for Internet crime still remains the criminal law in 1997 and the criminal law amendment in 2009 (VII). Although this situation has been changed to some extent in the amendment to the criminal law of the people's Republic of China (IX) on information network crime in 2015, in specific cases, the judge's judgment is still light for hackers who steal a large amount of personal data but do not make too much profit. To really promote the protection of data security, legislation should try to use data as the basis for judging the degree of crime, rather than just how much benefit these data have brought to criminals. Because the harm degree of data leakage should be paid enough attention. More importantly, although China has recently introduced the data security law of the people's Republic of China and the personal information protection law, there are no supporting laws and regulations to formulate corresponding solutions to specific problems, which will make such laws unable to play their due role. At the same time, as the Chinese leader said in his speech, there are not many systems, but refinement and pragmatism. Therefore, China's top priority on data protection is to establish the rigidity of the system and implement the requirements of the data security law of the people's Republic of China and the personal information protection law. If the problems of no supporting laws and the establishment of institutional rigidity can be solved, it will greatly promote the punishment mechanism for data intrusion, so as to promote the data protection of enterprises.

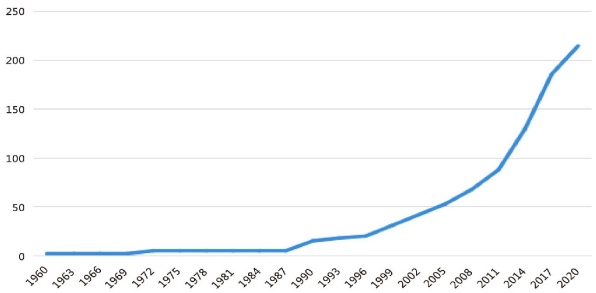

Figure 1. Number of cross-border data flow restrictions

5. CONCLUSION

Generally speaking, the problem of enterprise data protection is still a worldwide problem, and there are still many problems to be solved urgently. Moreover, due to the late start of Chinese laws in data protection, the weak supervision of enterprises and the insufficient attention of laws to data intrusion, China has been on the edge of the qualified line in data protection. Through the two case studies of Facebook and DiDi Global Inc. company, in order to solve the problem of enterprise data security protection, we must strengthen the legal supervision of enterprises in data protection and increase the legal punishment for data intrusion. At the same time, Chinese Personal Information Protection law and Data Security Law have been promulgated and gradually implemented. What China urgently needs to do now is to strengthen the supporting implementation connection of the system and establish the rigidity of the system. Only in this way can China better get rid of the legal dilemma in data protection and enter a new era of data protection. This article studies how to supervise data leakage in Chinese companies and what kind of supervision is used to protect the data or information rights of the corresponding subjects. As for the crime of data leakage, administrative punishment responsibilities and other

issues, it depends on the further research of relevant scholars.

REFERENCES

[1] Viktor Mayer-Schonberger, Kenneth Cukier, *The era of big data* , Zhejiang People's Press, pp.1-3

[2] Ma Zhongfa, Hu Ling, The Improvement of China's Legal System of Data Security Protection, vol.02, pp.1-75.

[3] Xue Yisa, *The Construction of the Multi-tier Outbound Data System and the Realization of Free Data Flowing:Starting with the Reform of the Substantive Review System*. Journal of Northwest University for Nationalities (Philosophy and Social Sciences Edition), vol.06, pp.64-74.

[4] Xiao Chengjun, Xu Yuzhen, *Personal Information Leakage and Multi-center Governance in the Era of Big Data.* Social Sciences in Inner Mongolia (Chinese Edition)), vol.02, pp.185-192.

[5] Yuan Wenxiu, Yu Hengxin, *Thinking about Information Ecology in Network Space*. Information Science, vol.01, pp.144-147.

[6] Wang Zhong, Yin Jianli, *Traceability Mechanism Design against Personal Data Privacy Disclosure under the Context of Big Data*. China Circulation Economy, vol.08, pp. 117-121.

[7] Li Lihong,*The Way to Protect Enterprise's Sensitive Data Leakage* . China Computer News. 2016-11-21(012).

[8] Wang Xiaoqun, et al., *Overview of My Country's Internet Security Situation in 2020*. Confidential Science and Technology, vol.05, pp.3-10.

[9] Hong Yanqing, *Regulation Based on Management:the Reconstruction of the Security Protection Obligations of Network Operators.* Global Legal Review, vol.04, pp. 20-40.

[10] Ulrich Beck, *Riskogesellschaft:Auf dem Weg in Eine Andere Moderne*. Yilin Press, pp. 38-44.

[11] Tao Qian, Song Chunyu, *Legal Governance Dilemma and Norm Application of Enterprise Data Leakage*. China Information Security, vol.05, pp.34-36.