Research on Security of Big Data in China

Jingxuan Wang*

Henan Experimental High School, Zhengzhou, Henan Province, China, 450002
**Corresponding author. Email: hasyzx@2008.sina.com*

ABSTRACT

In the contemporary society, we receive mountains of information moment by moment, Including television advertising and mobile phone advertising. What big data is doing is to find valuable information By the mass information. Users' privacy has met an unprecedented challenge. As a lot of new technologies emerge, the application of bug data faces more risks. So, this study mainly describes the current state of big data security, potential dangers, and regulatory issues. Finally, corresponding solutions to these potential dangers and regulatory issues are proposed. At present, the problem of imperfect data governance system and laws is becoming more and more serious. With the development of data decryption technique, they pose a serious threat to user privacy. Various advanced big data attack techniques, such as ATP attack technology, can make a self-protective stealthy attack. At present, my country has the following problems in data security governance: personal privacy is vulnerable to multivariate data association analysis and foreign infringement attacks; traditional security measures are difficult to meet current security requirements; the security mechanism of network platforms needs to be improved. Therefore, the Chinese government should further improve laws and regulations, deepen cooperation in the global digital economy, and develop advanced data protection technologies.

Keywords: *big data, data security governance, personal data protection*

1. INTRODUCTION

With the development of communication, artificial intelligence and other technologies, people's ability to acquire, transmit, store, process and apply information has been unprecedentedly improved. Especially in today's society with extremely inflated information, people rely more and more closely on information, so they have higher and higher requirements for the security of information system. This paper briefly reviews the potential risks of big data, focuses on the information chain carried by computers and network transmission, and provides some methods to ensure its security. This paper puts forward suggestions to strengthen data security governance in China, and provides solutions to the regulatory problems in data security governance in China, facilitating the formation of China's data governance system.

2. STATUS QUO OF BIG DATA SECURITY IN CHINA

2.1 The current status of China's current data security governance legal system

In fact, China is constantly formulating and improving data security governance systems to ensure the security of important data and personal data and give full play to their economic value." Network security Law", "Data Security Law", "Personal Information Protection Law" and "civil Code" all provide protection for data security.

2.2 The insufficiency of China's relevant data security law

Although China continues to formulate relevant laws and regulations, the system itself is too principled and lacks practicality and guidance. Taking The Data Security Law (Draft) as an example, the article 9 said that ‘The State supports the publicity and popularization of data security knowledge, improves the awareness and level of data security protection of the whole society, and

encourages relevant departments, industrial organizations, scientific research institutions, enterprises and individuals to participate in the work of data security protection'[1]. The collaborative governance system stipulated in Article 9 only defines the protection 2subject, but the implementation priorities and specific coordination are not clearly stated. Second, the Data Security Law (draft) has more systematic and comprehensive provisions on important data, but it does not specify the protected objects[2].

2.3 privacy leakage

Big data is a distributed system that can solve the higher level data storage problems to a certain extent. Similarly, from another point of view, big data is mainly used to analyze and apply some information, data, etc. At present, with the strengthening of various data decryption technologies, it will certainly pose a great threat to the privacy of some users. For example, nowadays, users of major communication software will leave some data in the process of utilization, but these data may be sorted out and stolen by some corresponding professionals. For example, people usually use mobile phones to locate and log in, which will leave some important information and data and will be collected by some market inspectors. The data obtained in this way not only has high accuracy, but also has a large amount of information. In China in 2021, there are billions of pieces of personal information obtained illegally and sold on the dark web for profits; Criminals obtained more than 2 million pieces of information about the elderly and defrauded more than 60 thousand elderly people of more than 15 million RMB; The criminals also registered game accounts and sold them to juveniles for profits of more than 1.7 million RMB[3]. Therefore, the security problems of big data are widespread in the market at present. In view of this situation, The security problems of big data are worth our deep consideration and urgent need to be improved and perfected.

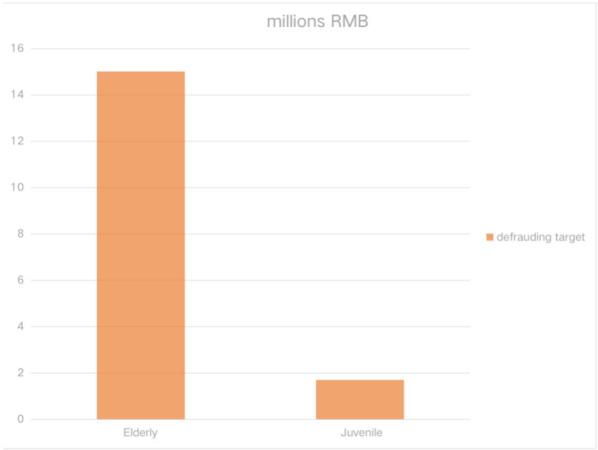

Figure 1. Two major internet defraud target in China in 2021

2.4 Long-term attack vehicle

Big data can serve as a vehicle for sustained attacks over a long period of time. Big data attacks have an advanced technology representative, referred to as APT attack technology, which is mainly characterized by a wide range of attack, large attack area, long attack time and good concealment. According to the survey, this is one of the technologies that big data is attracting people's attention in the security field. Compared with traditional attack technology, this kind of attack technology combines all kinds of most advanced means and social engineering, and can attack stealthily and self-protection. At present, big data attack technology has been widely used in the market. For example, hackers will use big data to launch attacks on the areas they want to attack. Such attacks can not only control a large number of objects at the same time, but also have an effect that traditional attack technology does not have. In 2006, Sykipot attacked vulnerabilities in Acrobat and Adobe Reader. It's part of a long-term series of cyber attack campaigns mainly aimed at U.S and U.K organizations including telecommunications companies, government departments and defence contractors. The attackers kept using targeted emails containing a link or malicious attachments containing a 0-day vulnerability. This kind of entry method is called spear-phishing, which is the most commonly used tactic in APT attacks[4].

3. PROBLEMS ENCOUNTERED IN BIG DATA SECURITY GOVERNANCE IN CHINA

3.1 Personal privacy protection

In the past, data was the asset of an enterprise and was used in the internal environment of the enterprise, which was not mobile, so personal privacy was not prominent. But now, the data is everywhere. All kinds of data information accumulated to form multivariate data association, and many attackers can lead to the disclosure of personal privacy information through multivariate data association analysis. How to effectively protect personal privacy is the first important issue facing big data security.

3.2 Cross-border data flows

In this day and age, the flow of data is important. The cross-border flow of data is a special attribute of big data. It is important to protect the security of cross-border data in terms of legal systems, data outsourcing, and fighting cyber crime. Therefore, when establishing the big data security standard system framework, it is necessary to analyze the applicability of all aspects of life cycle security standards such as traditional data collection, organization, storage, and processing. Then the appropriate ones need to be taken, the inappropriate ones modified, and the missing items added. Personal big data

security can easily be violated. For example: external unauthorized personnel maliciously invade information systems; illegally obtain private data, etc. After a data security incident occurs, effective traceability and audit cannot be performed. Big data requires flow and sharing, and the convergence and transmission of large amounts of data increases the risk of data leakage

3.3 traditional security measures' inelasticity

The characteristics of massive, multi-source, heterogeneous, and dynamic big data systems lead to complex storage structures, openness, distributed computing, and efficient and accurate services. These special requirements cannot be met by traditional security measures.

In the past, the traditional government governance generally implemented the one-way closed management mode, that is, adopted the bureaucratic management mode. With the passage of time, its disadvantages have become more and more prominent, mainly in the following aspects: First, qualitative and quantitative decisions are often emphasized in government decision-making, so these decisions are easily manipulated by empiricism, resulting in a high probability of decision-making mistakes. Moreover, policy formulation lacks transparency and does not meet the requirements of openness; Second, in public service, it passively responds to various needs of the public, which is inefficient and difficult to timely meet the personalized and urgent service requirements of the public; Third, in terms of social governance, the government and relevant functional departments mainly implement unified management, and lack of diversified collaborative governance, resulting in poor channels for social participation in governance, and the public's enthusiasm for participation is not high[5].

3.4 The platform security mechanism's shortage

We used to use ORACLE database, but in the era of big data, people are based on the Hadoop architecture. In hadoop architecture, security guarantee capabilities such as user identification and authorized access are relatively weak. At the same time, some open-source Hadoop components are not tested when they are used, and there may be loopholes and malicious codes, as well as back doors opened by others.

4. SUGGESTIONS ON DATA SECURITY GOVERNANCE IN CHINA

4.1 To further establish sound laws and regulations

4.1.1. Pass the Data Security Law as soon as possible

On July 3, 2020, the 20th meeting of the Standing Committee of the National People's Congress discussed the "Data Security Law (Draft)". After experts and scholars from all walks of life have extensively discussed and put forward many suggestions, the legislative department should synthesize useful opinions as soon as possible, formulate the "Data Security" as soon as possible, and indicate the direction of data protection.

4.1.2. Establish a relatively complete legal system as soon as possible

Although the relevant data security laws issued by China have a clear guiding ideology, there is no specific implementation of the lower law and relatively lacking in this respect. There is still a big gap from developed countries in Europe and the United States, so China should speed up the pace of legal construction. First of all, relevant departments should issue a law supporting the data security law as soon as possible. In response to various difficult issues, standardize the improvement, practicability and operability of the Cybersecurity Law and the Personal Information Protection Law. The second is to redefine data security protection standards. According to specific circumstances, key enterprises will be invited to participate in the formulation and improvement of safeguard standards and norms[6].

4.2 Deepen cooperation in the global digital economy

At present, China, the United States and Europe are the three core forces that will determine the future of the world's digital economy. First of all, the forum on China-Africa Cooperation, the Belt and Road Summit forum and other host diplomacy should be utilized to continuously enhance the influence of data security governance, vigorously promote China's propositions and suggestions, and accelerate the reach of world consensus. Second, actively participate in the formulation of international data security governance rules, give play to the role of the government and enterprises, and integrate Chinese suggestions into the world plan. Finally, we should strengthen multilateral cooperation, further expand consultations and negotiations, and reach consensus on a cyber community with a shared future as soon as possible.

4.3 Research and development of data security technology

Science and technology are the basis for ensuring data security. The UK invested £189m in big data technology in 2013 and another £73m in 2014.The U.S. cyber defense system was introduced to Japan in 2014.The United States has launched a number of big data research strategic projects. Developed countries in Europe and the United States are actively developing key core technologies of big data[7].

5. CONCLUSION

This study focuses on the big data security issues in China, including the status quo, current problems and some suggestions. At present, China has made continuous progress in legislation, but the system lacks practicality and guidance. With the development of data decryption technique, it, poses a serious threat to user privacy. Big data can serve as a vehicle for sustained attacks over a long period of time. For information security governance, we encounter the following problems: Personal privacy is vulnerable to attacks by multivariate data association analysis and foreign infringement. Traditional security measures are difficult to meet security requirement. To this end, the author puts forward the following suggestions: relevant departments should further improve laws and regulations; and deeply participate in global digital economic cooperation, research and development of data security technology, etc. The main limitation of this study is the lack of reliable data from the study. In terms of big data security governance, China still has a long way to go. This study provides recommendations for the current situation only. More needs to be done to ensure information security or cybersecurity in a more efficient and practical way.

REFERENCES

[1] Data security law of the People’s Republic of China

[2] Ma ZhongFa/Hu Ling, The improvement of China's Legal system of Data Security Protection, Law School, Fudan University, 2021, Page 5

[3] Billions of messages stolen! The Ministry of Public Security announced the top 10 typical cases of infringement of personal information in 2021. https://m.thepaper.cn/baijiahao_16452308

[4] Five notable examples of advanced persistent threat (APT) attacks. https://www.getsafeonline.org/business/blog-item/five-notable-examples-of-advanced-persistent-threat-apt-attacks/#:~:text=Some%20of%20the%20most%20notable%2021%20st%20century,an%20operation%20nicknamed%20Titan%20Rain%20by%20U.S%20investigators.

[5] Liao Zhenmin, Big data Governance: A revolutionary approach to traditional government governance, 2018, Page 2

[6] Jing'jing Shao/Xiao'feng Han, Overview of data security governance at home and Abroad, Journal of information Security Research, 2021, Page 9

[7] Zhou JiLi/Li DeBin, Major experience and enlightenment of foreign big data security development, Page 5