Advances in Social Science, Education and Humanities Research, volume 290

2nd International Conference on Economic Development and Education Management (ICEDEM 2018)

Research on Data Security Ecosystem Construction Based on Big Data Background

Rui Ma[1,a], Qiong-juan Wen[1,b],* , Hong-zhen Lin[1,c], Yun-jun Jiang[1,d]

[1]School of Hengda Management, Wuhan University of Science and Technology

947 He Ping Street, Hubei Wuhan 430081, China

[a]1057607653@qq.com, [b]5438227@qq.com, [c]996672199@qq.com, [d]1499896794@qq.com

***Abstract*—The purpose of this paper is to study how to build a data security ecosystem in the context of big data and promote the scientific and sound development of China's big data industry. By means of literature investigation and comparison, this paper makes a comparative study on the development status of international and domestic data security, and puts forward feasible suggestions for the reasonable construction of China's data security ecosystem. In the age of current information, it is driven by The Times to create more beneficial development mode based on the potential value of big data. But the development of the basic premise is to ensure the safety of data, this paper on the basis of comprehensive analysis on the data security in our country development present situation, proposed that the parties involved should take necessary measures, and the conclusion is that based on the background of big data, in order to promote the sound development of the economy and promote the necessary way of maintaining the order of social and economic development is to build a data security ecosystem composed of four parts: country, industry, enterprise and individual.**

Keywords—Data security; The ecosystem; Build; Coordinate

I. INTRODUCTION

In recent years, with the development of social economy, The change and development of information technology is also hastening the arrival of the era of big data. From personal information to state secrets, they are being collected and used to analyze and explore their potential value, and to build a better blueprint for the future development of human beings and society. However, at present, the development of big data in China is still in the preliminary stage, which lacks a lot of theoretical guidance and practical experience. At the same time, some lawbreakers attempt to make profits through big data, leading to numerous information leakage and data theft incidents of the public, which has a great negative impact on the society.

According to a survey by the Ponemon Institute, agencies are estimated to lose an average of $200 for every piece of information they lose. For each full data breach, the average loss would be as high as $6.8 million. [1] Thus it can be seen that the loss caused by data leakage is huge, Therefore, it is imperative to guarantee the data security of all parties in such an information era in the context of big data. "Building a data security ecosystem based on the big data background" is the starting point of this paper. By giving the definition of data security under the big data background, this paper analyzes the current status of China's data security development from four participating subjects: the state, industry, enterprises and individuals, and gives the necessary measures for the construction of the data security ecosystem.

II. NECESSITY OF BUILDING A DATA SECURITY ECOSYSTEM

A. Promoting the protection of personal privacy

In the information age under the context of big data, data is undoubtedly the most important resource. Ensuring data security is a necessary prerequisite for data value mining. Countries are also constantly updating the definition and processing standards of personal data, For example, the European Union's GDPR, known as the strictest personal data protection regulation in history, On the one hand, on the basis of expanding the meaning of personal data, the concept of pseudonymous data is also introduced. At the same time, the data processing rights such as the right of access, the right of being forgotten, the right of restricting processing and the right of data migration are clearly regulated and defined. [2] On June 1, 2017, China implemented *the cyber security law of the People's Republic of China*, and on May 1, 2018, China formally implemented *the personal information security specification of information security technology*, which aims to crack down on illegal collection, abuse and leakage of personal information, and to protect the legitimate rights of individuals and the public. To sum up, based on existing literature, this paper defines data security in the context of big data as follows: in the process of value mining with big data, the confidentiality, integrity and availability requirements of personal information and data shall be fully guaranteed.

B. Promoting data security

In the era of big data, to truly guarantee data security, all parties need to actively participate in order to promote healthy and sound development of data security. Tansley for the first time in 1935 formally put forward "ecosystem" . It refers to the unity formed by the interaction between producers, consumers, disintegrators and non-biological substances and energies within a certain time and space range. [3] This paper constructs a "four-in-one" data security ecosystem composed of countries, industries, enterprises and individuals, and makes clear specifications of data collection, storage, encryption, prediction, analysis and utilization. Meanwhile, it strengthens the dynamic

connection and maintenance of all parties, and promotes the completion of data security development.

III. Analysis of the Problems of data security development in China

A. Imperfect law

China has been concerned about computer data security since the early 1990s and has implemented relevant regulations and provisions. Keeping up with the time development , many laws and regulations related to network data security and personal privacy protection have been issued in China, but their subjectivity is still weak, and the relevant core regulations are not specific and complete enough. At present, China's laws and regulations are only protected from the perspective of personality rights. Regulatory bodies lacks functional division, coordination and communication, and wastes administrative resources, so that personal information security cannot be effectively supervised [4]. Therefore, compared with frequent data security incidents and increasing data security vulnerabilities, related laws in China are still inadequate in terms of systematisms, timeliness and legislative specifications. Since the formulation, the promotion and implementation intensity and implementation feedback effect in various parts of the country are relatively satisfactory.

B. Lack of industrial autonomy

At present, almost all Internet industries in China are faced with data security problems, especially those directly connected with user groups, such as medical care, electronic communication and e-commerce. Since the 18th national congress of the communist party of China, the application of big data has had a certain degree of influence in many industries of China's real economy. The mining, cross-integration and sharing of data information resources in the industry has brought a lot of convenience to the common development of the industry as a whole. However, in the process of sharing data information resources, the lack of standardized data security control system and sound data protection technology in multiple links such as data mining management, information integration and data analysis and utilization, as well as the separation of ownership and right to use of big data has made it increasingly frequent that users or enterprises suffer serious economic losses due to the increase of data abuse or personal privacy security risks in the industry.

C. Prevention awareness of enterprise is not in place

With the development of China's e-commerce industry gradually entering the mature stage, big data technology is more and more widely used for business purposes, such as obtaining users' personal information and analyzing consumers' behavior habits, so as to achieve the targeted target groups for precision marketing. The mining, classification, integration and analysis of data information are becoming more and more convenient in today's society with the rapid development of information technology, but it cannot be ignored that the data security protection technology used by most enterprises is not sound enough. While legitimate users of data use big data technology to collect, analyze and mine valuable information, attackers can also use big data technology to obtain the desired information to the maximum extent, increasing the risk of leakage of sensitive information by enterprises. [5] Judging from the actual management of Chinese enterprises in data safety prevention, many enterprises are lack of foresight for the occurrence of data safety accidents, and have not established the data safety prevention mechanism or the existing prevention mechanism in a single form, which lacks flexibility.

D. Lack of personal data security awareness

With the deepening of social informatization, people's common use of the network is embodied in the fervor of mobile social network. However, mobile social networks are faced with information security problems while providing users with ubiquitous information content. According to a new survey from security software company Webroot, users of social networking sites are more likely to encounter security threats such as loss of financial information, stolen identity information and malware infections ,which maybe more serious than they think[6]. On the one hand, with the advent of the era of big data, various online behaviors of the public are monitored in real time. While the development of science and technology brings people pleasure and convenience, it also stealthily sneaks into people's private life. Once social software is attacked by foreign malicious viruses, hundreds of millions of citizens' data information will be exposed to the Internet, bringing huge losses to people and society. On the other hand, the low awareness of users' personal data security protection also aggravates the frequency of data leakage incidents. For example, users always input personal key information without precaution while downloading various software in the app store, and they often attach the same phone number or email address when setting their account. At the same time, users also lack the necessary awareness and action after data leakage [7].

IV. Measures to build a data security ecosystem

A. Measures Of The National Level

The urgent need of data security governance in economic society cannot be solved without strict regulation and policy support. Therefore, the formulation of relevant draft laws on data security and user privacy protection and the improvement of data management mechanism have become effective measures to guarantee the development and reasonable utilization of enterprise data security and avoid loss caused by personal data leakage under the background of big data. [8] Secondly, the government should actively cultivate technical talents and promote the development of data security technology. For example, the government can cooperate with universities to set up courses related to big data, data security technology, etc., to raise students' attention to data security under the background of big data and strongly support universities to cultivate talents in the field of data security technology. Big data is the product of the rapid development of information technology, and at the same time, it puts forward higher requirements for the development level of information technology. Therefore, the government's encouraging policies, including financial investment and other aspects of support, are

also indispensable for promoting the continuous improvement of the overall technical level of data security in society.

B. Measures Of the industry level

As the application development of big data in various industries of China's real economy has just started, it is difficult to control the balance between data sharing and data resource protection. Every time data sharing is carried out in the industry, it will add a risk and security hidden danger to the leakage of data information resources. Therefore, the industry should establish a standard and reasonable industrial data security control system. First, the industry as a whole should draw up rules and regulations related to data sharing security, strengthen self-restraint within the industry and strengthen the protection of data resources. Secondly, we can build a data security monitoring mechanism in the whole industry and establish a third-party technical monitoring department in cooperation with relevant government departments. So that they can register and record the enterprises that participate in the data sharing in the industry and carry out regular safety inspection and legality monitoring on the data collection system of enterprises in the industry, and regulate the industry data mining and sharing technology. Only with the establishment of a standardized industry data security control system and strong technical support, can the industry jointly fully explore the inherent value behind big data and create a "win-win" good development model.

C. Measures of the enterprise level

In the era of big data, it is particularly important to establish a perfect data security management system for enterprise data security protection. After analyzing the actual situation of Chinese Internet enterprises, it should be established from the following aspects. First of all, enterprises should formulate rules and regulations related to big data security, and mine and integrate data resources with the basic principles of legality, legitimacy and necessity. According to the data security laws and regulations issued by the state, enterprises can standardize the means of data security protection based on their actual operating conditions to avoid serious losses of enterprises and users caused by data leakage. Secondly, the enterprise ecosystem based on "big data" must build advanced infrastructure, build a good data processing and knowledge sharing environment, and unblock the data communication channels of the enterprise ecosystem, so as to form the core assets of "big data" and improve the transfer and application benefits of "big data". [9]

D. Measures of the individual level

As the most important participant in the data security ecosystem, the public's role in it cannot be ignored. First, the information security literacy should be improved. Improving information security literacy is a powerful measure for social network users to actively protect personal information security in the era of big data. Specifically, information security literacy includes information security awareness, information security knowledge, information ethics and information security capabilities [10]. In daily life, users should have a certain ability of discrimination before using the application software, and think rationally whether they will operate their own information improperly. At the same time, users should be alert when registering, avoid binding with the same mobile phone number or mailbox for a long time, and fully consider whether it is easy to be broken when setting the password. Finally, in daily life, we should pay more attention to the latest news and policy interpretation of information security and data leakage, so as to enhance our awareness of data security and information protection.

V. CONCLUSION

The advent of the era of big data is driven by The Times. In the current context, it is imperative to build a data security ecosystem composed of four "integration" of countries, industries, enterprises and individuals. Based on the existing literature and data research and by analyzing the current development status of China's data security field, this article proposes the meaning of data security in the context of big data and the necessary measures for the construction of data security ecosystem, aiming to guide the participants to better mine the value of data and information through the construction of theoretical models and create greater value for human and society.

ACKNOWLEDGEMENT

This study was funded by the 2018 hubei university students innovation and entrepreneurship training program project: research on data security ecosystem construction in the context of big data, no. :201810488056.

REFERENCES

[1] Five ways to prevent data leakage in smes[J]. Computer and network,2013(2): 50. (In Chinese)

[2] Liu Yaohua, Lin lin. How should China deal with the implementation of GDPR[J]. Information and communications technology and policy,2018(09):74-77. (In Chinese)

[3] Tansley A G. The use and abuse of vegetational concepts and terms[J]. Ecology,1935,16(3):284-307.

[4] Zhao Anqi. How does personal information security realize rule of law sharing in the era of big data [J]. Legal expo,2018 (29): 119. (In Chinese)

[5] Lu Litao, Li Chuxiong. New features and requirements of enterprise information security in the era of big data [J]. Electronic technology and software engineering,2018 (12): 226. (In Chinese)

[6] Wang na, Xu Dachen. Investigation and analysis of personal information protection in mobile social network [J]. Digital LAN, 2015(01):185-194. (In Chinese)

[7] Zhang Yanxin, Kang Xu ran. Research on personal information security of social networks in the age of big data [J]. Digital LAN,2014(05):24-25. (In Chinese)

[8] Zheng Yin. Research on the guarantee mechanism of government data opening and utilization in the era of big data [J]. Journal of agricultural books and information,2018,30(10): 87-90. (In Chinese)

[9] Zi Wucheng. The evolution and construction of enterprise ecosystem in the era of "big data"[J]. The social sciences,2013(12). (In Chinese)

[10] Luo Li. Research on the construction of national information security literacy evaluation index system[J]. journal of chongqing university,2012(3). (In Chinese)