Research on Network Data Security Management in the Age of Big Data

Cheng Yan

Department of Computer Science and Engineering, East China University of Political Science and Law, Shanghai, China

chengyan@ecupl.edu.cn

Keywords: Big data, Network data, Security management.

Abstract. In the era of "big data", the deep integration of big data into various fields has broken the boundaries between many industries. The "blowout" growth of network data has made the security protection of network data more complicated. Based on the comparison of domestic and foreign big data management ideas and legislative protection status, this paper expounds the counter-measures of data security management for the retention and sharing of network data in China.

1. Introduction

Network data was defined for the first time in Network Security Law of the People's Republic of China (Draft) issued in 2015, which refers to various electronic data collected, stored, transmitted, processed and generated through the network, such as various types of Emails, videos, voices, photos, profiles or social network messages circulated on the Internet. The openness of the Internet has made various types of data semi-open basically, and "network data sharing" has become the mainstream attitude of international network data usage. Especially in the era of "big data", the deep integration of "Internet +" with government, medical, financial and other fields has created a new impetus for economic development, and broken the boundaries between many industries. The "blowout" growth of network data has made network data security protection more complicated and brought more severe challenges to data security.

Firstly, network big data storage types are more complex, including structured, unstructured, semi-structured and many other types. Unstructured data imposes new requirements on big data encryption storage;

Secondly, the development of "big data" further improves the openness of information. The opening of government-controlled data, which is related to people's livelihood and does not involve personal privacy and state secrets, helps to expand the big data industry and create new formats. However, due to the huge information underlying in the network big data, the fragmented information that originally appeared "scattered distribution" is gathered together, and after specific analysis and processing, is likely to reveal personal privacy and sensitive information of the state or some special departments, increasing the security risks of internetwork cooperation and data sharing.

Thirdly, in the context of big data, many service providers like Tencent, Weibo and etc. are not only data producers, but also data storage, managers and users. Thus, it is difficult to achieve security protection of data or privacy simply by restricting the use of network data through technical means.

Before the "prism" incident, the openness of network data was increasingly deepening, and data cooperation, mining, and analysis between nations, enterprises as well as governments and enterprises continued to put forward. However, after the "prism" incident, countries began to notice the importance of network data protection and strengthen the security management of network data.

2. International comparison of big data security protection legislation

The research on security management of network big data first emerged in western countries. The international community is carrying out data security assurance practices from three aspects including technology protection, enterprise management and laws and regulations. In a nutshell, through well-designed network architecture and data backup mechanism, improved hardware device

  DOI: 10.25236/iwmecs.2019.115

performance, upgraded firewall technology and data encryption technology, technology protection can deal with emergencies such as physical equipment failures, virus outbreaks, hacker attacks and etc.. From the management's point of view, enterprises should strengthen the monitoring of data modification, inquiries, copying and etc., and prohibit employees from disclosing customer information and other data by signing confidentiality agreements and developing internal regulations. However, due to lack of clear and powerful punishment principles, leak of data information is of low illegal cost. Therefore, it is necessary to formulate corresponding laws and regulations, strategic policies, management standards and etc. at the national level to supervise and constrain enterprises and maintain the data security of the government, the Department of Defense, enterprises and etc..

In March 2012, US President Obama announced the launch of the "Big Data R&D Program", which invested more than $200 million to fund research and development of new projects to improve the core technologies needed to collect, store, retain, manage, analyze and share mass data. At present, many western countries adopted a management model government-led supervision combining with data security technology, enacting and improve laws and regulations related to big data, The government established organizations specializing in data protection, providing strong legislative guarantees for the network data security in accordance with strategies and regulations at the national level, such as the Federal Data Protection Committee of Germany, the Data Protection Agency of the Netherlands, the Ministry of Administrative Security and the Communications Commission of South Korea.

In terms of the timeliness of data retention, UK 2014 Data Retention and Investigation Rights Act Amendments imposed mandatory legal requirements for data retention, requiring communication service providers to retain user communication data for 12 months and disclose at legal claim made by law enforcers. In October 2015, Australia passed Telecommunications (Monitoring and Access) Amendment (Data Retention) Proposal, requiring Telecom operators to retain data of telephone, Internet, and e-mail users for two years. In terms of data sharing, UK released the Open Data White Paper in 2012, promoting the opening of public service data; and published Obtaining the Opportunities Brought by Data: The UK Data Capability Strategy published in 2013, developed measures including improving data analysis techniques, strengthening state infrastructure construction, promoting cooperation between research and industries, and ensuring secure data access and sharing. In order to deal with the risks arising in data sharing, Russia issued Information, Information Technology and Information Protection in 2015, stipulating that the personal data of Russian citizens can only be stored in domestic servers to ensure data localization.

EU General Data Protection Regulations (GDPR) issued on May 25, 2018 was referred to by the industry as the "most stringent" data information protection regulation. The regulations have "overload penalty" and "the broadest jurisdiction". From the user's point of view, GDPR definitely protects users' privacy, while from the perspective of the company, GDPR's cost is much higher than the return from the European market in one or two years, which keeps many small and medium-sized companies away.

In China, although more and more enterprises and organizations have been aware of the network data security issue, laws and regulations on data security management are not formulated systematically. In terms of data retention, Provisions on the Technical Measures for the Protection of the Security of the Internet, Administrative Measures for Internet Information Services and Provisions on the Administration of Online Publishing Services stipulate that users' network data should be retained for at least 60 days, while Administrative Measures for Online Trading stipulates that users' data should be retained no less than two years. In recent years, a series of policies and regulations on protecting the personal information of users have been issued. In Provisions on Protecting the Personal Information of Telecommunications and Internet Users, Definition and Classification of Personal Information Protection for Telecommunications and Internet Service Users and Guidelines for the Classification of Personal Information Protection for Telecommunications and Internet Service Users approved and issued by the Ministry of Industry and Information Technology, network data is under classified and graded protection based on its sensitivity, and appropriate

security protection measures are taken in accordance with Administrative Measures for the Graded Protection of Information Security. Provisions on Strengthening Network Information Protection, Cybersecurity Law, Provisions on the Technical Measures for the Protection of the Security of the Internet and Administrative Measures for Online Trading clearly stipulate that corporate users should ask users to provide real identity information when providing services such as network access, information release and etc.. The existing information security or user personal information protection is not well suited to the conditions of big data, and old problems have not been resolved while new problems are emerging. In terms of data sharing, the Measures for the Administration of Population Health Information (for Trial Implementation), Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions, and Notice of People's Bank of China on Banks and Financial Institutions Protecting Personal Financial Information all explicitly prohibit transferring network data involving users' sensitive personal information abroad. The latest version of Cybersecurity Law clearly stipulates that operators of critical information infrastructure that have not conducted security assessments may not store abroad or transfer important information such as citizens' information collected and generated in operations. In some specific industry sectors, there is still a lack of regulations and supervision over the collection, storage, management and use of network data. At present, it still relies on the self-discipline of enterprises. Some enterprises such as China Telecom and China Unicom have already established internal rules and regulations on network data management, but there is still no laws and regulations at the state level.

3. Research on Big Data Security Management Countermeasures

China's Internet development environment is very different from that of developed countries such as the United States and the European Union. The government is currently facing the challenges of balancing the relationship between network security, data protection and economic development. The characteristic of big data is to realize the circulation and sharing of data, and promote effective collaboration between governments and enterprises in the Internet age. Although we cannot copy the experience and methods of foreign countries, we can refer to industry self-discipline or legislation-based protection of foreign countries and provide new perspectives and methods for network data security protection in China.

(1) Formulating rules for standardized management of big data

In the era of big data, network data is of large amount and diverse data sources, including various structured, unstructured and semi-structured data such as databases, texts, pictures, videos, and web pages. The government should formulate unified data management standards and rules, possibly including data specifications and standards, data quality management measures, data management organizations and responsibility systems, data security management measures, data usage management measures and etc.. Information system developers should design and implement data architecture, model, storage form, and flow mode under the guidance of the specifications. When the information system is delivered and used, the data user should not only upgrade the data security core technology, but also have supporting internal regulations to implement data security and standardized management.

(2) Strengthen the regulatory mechanism of big data entities

Entities having big data such as government and enterprises are also crucial to data management and protection. In addition to monitoring data security through technical means and continuously upgrading core data security technologies, enterprises or departments must also formulate bylaws to realized standardized management on collection and storage of big data, and supervision over data sharing and use. For example, enterprises can set up a special data management organization, department or position, which takes responsibility for the management and security monitoring of all data, and make unified planning for the data structure, model, storage, circulation, use and etc.. i.e. classify all stored data by security level according to the type and storage requirements of network big data and apply different management measures in terms of encryption storage, disaster recovery and

etc., formulate and control the rules for backup, storage and use of the data information, ensuring sharing and effective use of data in the entity.

(3) Establish a government-led data sharing platform

In order to effectively realize data integration and sharing and meet the requirements of high-quality data management, a government-led standardized data sharing platform must be established, which is responsible for the establishment and subsequent management of the data sharing management platform. It involves the formulation and implementation of mechanisms regarding data storage and backup, data sharing, and shared entity rights and responsibilities.

1) Data storage and backup mechanism: There are various kinds of data resources on the sharing platform and their sensitivity degree and risks faced are not the same under different application requirements. How to set a standardized format for data storage, how to design sensitivity standards, and classify security levels based on the sensitivity of the data (especially risk assessment of cross-border data flow), set user authorization, access monitoring permissions and retention period and etc., are key consideration for strengthening data storage and backup specifications.

2) Data sharing mechanism: establish a shared data list, specify the content and type of shareable data, limited shareable data and data that is prohibited to be shared; clarify the definition and scope of private information, and for shareable and transferable data, set information privacy classification rules according to its sensitivity to achieve the standardization of network interconnection, data integration, and resource sharing processes for various levels and types of information systems. We can classify all the data entities into three types: data managers, data suppliers and data users. Define the rights and responsibilities of them and develop the behavior constraints and accountability policies.

3) Rights and responsibilities of data sharing entities: In the process of big data sharing, data operators, such as mobile operators, banks, cross-border e-commerce, civil aviation enterprises, search engines, social media and other big data entities, have multiple identities. They are both data owner and data processor. The author believes that in order to achieve effective supervision and management on all links in the data sharing industry chain, it is necessary to standardize the data sharing process of all data entities, and according to the different roles of data entities, establish the rights and obligations as well as accountability mechanisms in terms of data acquisition, use and management on the data sharing platform.

4. Conclusion

In the era of big data, the development of Internet technology has brought more serious challenges to data security. It is difficult to achieve the security protection of data or privacy by limiting big data entities in the management and use of network data merely through technical means, and it is also not in line with the characteristics of openness and shared applications of network data. Only by establishing data sharing platforms, developing sound network data security protection systems and strengthening the big data security monitoring evaluation procedures and management mechanisms from the legislative level, can we effectively improve the integrity, confidentiality and availability of network data in the context of big data, and promote the process of building China into a network power.

Acknowledgement

This research was financially supported by the Ministry of Education of Humanities and Social Science project (17YJCZH031).

References

[1] Aoying Zhou, Cheqing Jin, Guoren Wang, A Survey on the Management of Uncertain Data, Chinese Journal of Computers, vol.2, No.1, 2009

[2] EMC, RSA, White Paper, 2013 [EB/OL]. http://korea.emc.com/collateral/white-papers/h0812-getting-real-security-management-big-data-wp.pdf

[3] Feng Dengguo, Zhang Min, Li hao, Big Data Security and Privacy Protection, Chinese Journal of Computers, vol.37, No.1, 2014

[4] Yu Hao, The opportunity, challenges and solutions of the management of government data in the age of big data, No.3,2015

[5] Information on http://www.cac.gov.cn/