ISSN 2522-3488 Vol. 7, Issue 2: 59-63, DOI: 10.25236/IJNDES.2023.070210

Research on Personal Information Security Protection Measures in the Big Data Era

Jiana Bi[1,*], Yonghong Guo[1], Ning He[1], Shuang Wang[2]

[1]*School of Software and Big Data, Changzhou College of Information Technology, Changzhou, China*
[2]*School of Physical Education, Bohai University, Jinzhou, China*
544099426@qq.com
[*]*Corresponding author*

Abstract: *While big data brings convenience to people, it also exposes various problems. Personal information is always exposed to risks. Protecting personal information from infringement in the big data era has become an urgent problem to be solved. This paper studies from three aspects. First, it analyzes the importance of personal information security protection in the big dataera: maintaining normal social production and life order, protecting personal physical and mental health and property safety, and reducing the occurrence of cyber crimes. Second, it summarizes the problems existing in personal information security protection in the big data era: serious disclosure of personal privacy information, malicious attacks on personal privacy by cyber hackers, low awareness of personal information security protection, and imperfect laws and regulations on personal information security protection. Third, the main measures of personal information security protection in the big data eraare put forward: improving the laws and regulations of personal information protection, raising the awareness of personal information security protection, building a data-centric security governance system, and strengthening the prevention and governance of cyber hacking attacks.*

Keywords: *Big Data Era; Personal Information Security; Existing Problems; Protective Measures*

1. Introduction

Nowadays, scientific and technological progress is advancing by leaps and bounds. Modern information technologies such as the Internet, cloud computing and big data have profoundly changed the way people think, produce, live and learn, and profoundly demonstrated the prospect of world development. The world has entered a data-driven era.Big data provides effective data support for social development, business forecasting and scientific progress, and is the basis of data services. There are more and more data about personal information in big data, which not only contains personal basic information, but also contains various related information. Analyzing and searching information from big data environment has become the main channel for personal information theft [1].Personal information in the era of big data includes the following three types. First, information reflecting personal natural conditions and social life background, including names and identities; Second, the traces left by individuals in the big data environment, including web browsing and shopping information; Third, the personal information generated by network service providers through the analysis and integration of the above two kinds of information, including personal interest orientation, shopping intention and browsing habits.

The above three kinds of personal information are both private and non-private. The boundary of privacy is not objectively fixed, but influenced by multiple factors. In the era of big data, the "fair use" of personal information is advocated, and "fair use" constitutes the boundary of privacy. Whether the personal information is handled reasonably depends on whether the impact can be accepted by individuals and whether it meets their reasonable expectations.Big data has the characteristics of large capacity, fast processing speed, various data types and low data value density, which also promotes the massive data to be processed and utilized in different ways.While big data brings convenience to people, it also exposes various problems. Information is excessively collected, and personal information is always exposed. Some lawless elements will also use online data to commit crimes, not only for the parties, but also seriously endangering social order and stability. Protecting personal information from infringement in the era of big data has become an urgent problem to be solved. In this context, the research of this topic will provide effective measures for personal information security

ISSN 2522-3488 Vol. 7, Issue 2: 59-63, DOI: 10.25236/IJNDES.2023.070210

protection in the era of big data.

2. Importance of Personal Information Security Protection in the Big Data Era

2.1 Maintaining normal social production and life order.

In the big data era, personal information security protection should also follow the principle of "safety first" [2]. Reasonable and moderate advertising push can meet consumers' potential shopping needs and get consumers' acceptance and recognition under the condition of relatively balanced information between buyers and sellers.However, if excessive advertisements are placed, the normal life and work order of consumers will inevitably be disturbed by advertisements that jump out of order. If this kind of bad publicity mode is normalized or popularized, the whole consumption format will tend to deteriorate, which will have a serious negative impact on consumers, businesses or service industries and affect the normal society production and life order.

2.2 Protecting personal physical and mental health and property safety

Various text propaganda contents and short video images, as well as anti-fraud propaganda, have become hot spots in online and offline communication. The harm of telecom fraud has gone beyond the scope of citizens' property safety and affected the deeper level of physical and mental health.Especially for the elderly and inexperienced minors who lack basic knowledge of the internet, losing money after being defrauded will often be accompanied by extremely serious psychological harm, which violates the moral and legal requirements for protecting the vulnerable groups in society. Doing a good job in personal information security protection and preventing various hazards including telecom fraud is to protect personal physical and mental health and property safety.

2.3 Reducing the occurrence of cyber crimes

The main purpose of cybercrime is to obtain personal information through improper means and commit crimes on the basis of this information. For example, criminals use Trojans to attack users' computers, obtain users' online banking information, and use the balance to buy funds. The funds in users' online banking will be taken away, and then they will contact users to obtain verification codes by deception. If users fail to see through this scam and tell each other about the operation verification codes, the money will be gone [3].If the user's personal information is effectively protected, hackers can't attack the user's personal system, or they can't get personal information by attacking the personal system, and these problems will not happen. Therefore, protecting users' personal information is an effective means to reduce cybercrimes.

3. Problems in Personal Information Security Protection in the Big Data Era

3.1 Serious disclosure of personal privacy information

With the popularity of smart devices such as smart phones, sports watches and smart bracelets, a large number of smart apps appear in daily life, which not only facilitates people's lives, but also causes great harm to personal information security.While collecting the necessary data for operation, various mobile apps often collect a large amount of personal privacy data completely unrelated to their functions, including location information, call records, address books, microphone monitoring and camera calls.Many "rogue apps" steal all kinds of user information, reveal users' privacy, and sell users' personal data, resulting in long-term illegal activities such as sales promotion and fraud. In the era of big data, personal privacy data has been completely out of the control of users.

3.2 Malicious attacks on personal privacy by cyber hackers

Hackers refer to people who wander in the network and break down their obstacles. Hacking methods can be divided into two types: non-destructive attacks and destructive attacks.Non-destructive attacks are generally aimed at disrupting the operation of the system and do not steal system data. Denial of service attacks or information bombs are usually used. Destructive attacks are aimed at invading other people's computer systems, stealing confidential information of systems and destroying data of target systems.In the big data era, hackers show new characteristics in attack means, attack

ISSN 2522-3488 Vol. 7, Issue 2: 59-63, DOI: 10.25236/IJNDES.2023.070210

methods, attack scope and attack psychology, which makes the current network security threats continue to increase and personal information leaks increasingly frequent, bringing new challenges to network security and network governance [4].

3.3 Low awareness of personal information security protection

Personal information protection consciousness is not strong, which has caused information leakage to some extent. Many people lack the necessary safety awareness of their own private information, and are insensitive to most private data. They will leak their personal information intentionally or unintentionally at ordinary times, which greatly reduces the cost for offenders to obtain personal privacy information [5].At the same time, some of their own behaviors are also intentionally or unintentionally infringing on others' personal privacy, thus indirectly becoming accomplices of offenders. Many netizens have poor awareness of privacy protection, and there is a phenomenon of arbitrarily authorizing personal privacy rights.Some mobile Apps are constantly making small moves, evading supervision in various ways, stealing user information, excessively demanding application rights, and collecting user information to achieve the purpose of "monitoring" users.

3.4 Imperfect laws and regulations on personal information security protection

Although *China's Criminal Law*, *General Principles of Civil Law*, *Cyber Security Law* and other important legal documents have partial designs on personal information protection, it is still difficult to bear the burden of personal information protection law, which leaves an opportunity for criminals [6].As a basic law, its main function is to provide direction guidance and ideas for all participants in network security through general expression, rather than solving specific problems, so it is difficult to avoid the characteristics of too principled provisions.Talking about personal information protection from the perspective of network information security can't avoid being abstract or scattered. What personal information can flow or be used? What personal information must be kept confidential? How to determine the data property rights of users? All these need to be clarified by a legal system.

4. The Main Measures of Personal Information Security Protection in the Big Data Era

4.1 Improving the laws and regulations of personal information protection

At this stage, it is necessary to formulate relatively perfect laws and regulations for new problems arising under the background of big data, to protect citizens' personal information from being leaked, and to reduce personal property losses and physical and mental health damage [7].On the basis of emphasizing the responsibility of institutions or data subjects represented by government departments, enterprises and institutions, network operators, network product service providers and related industry units, it further provides legal protection for individuals to effectively exercise their right to know, delete and correct.Take the protection of personal information as an important system, and strengthen the protection responsibility of the subjects who collect and use personal information. When collecting or using personal information, network operators should follow the principles of legality, justness and necessity, disclose the purpose, manner and scope of using information, and obtain the consent of the collected person.It is necessary to constantly improve the laws and regulations related to personal information protection, make full use of the advantages of big data technology, clarify the right to personal information and the right to independent personality at the legislative level, stipulate the compensation system for personal information rights infringement at the civil level, increase penalties at the criminal legislative level, enhance the awareness of personal information rights protection, and ensure the benign use of information under the background of big data.

4.2 Raising the awareness of personal information security protection

The main body of network security threats is individuals. No matter how perfect the network security technology and the legal system are, the threat of information disclosure cannot be completely eliminated [8].Therefore, individuals must improve their awareness of information security protection, learn to distinguish useful information, useless information and harmful information, and improve their ability to distinguish negative information and their awareness of self-protection; We should learn to cultivate the ability of obtaining information, processing information, applying information and information immunity.

ISSN 2522-3488 Vol. 7, Issue 2: 59-63, DOI: 10.25236/IJNDES.2023.070210

4.3 Building a data-centric security governance system

For the country, it is necessary to carry out top-level design, strive to build a cyberspace data security guarantee system that keeps pace with the times, and strive to realize the strategic transformation from response to active protection, so as to safeguard national cyberspace security, which is directly related to national security and people's interests, and to the national strategic needs of serving key information infrastructure and important information systems.For enterprises or organizations, data security governance is related to asset security and sustainable development strategy, and data security protection must be done from the aspects of protecting business secrets, business security and customer rights and interests.First, protect the security of data itself, including confidentiality, integrity and availability. Second, meet the compliance requirements of relevant national laws and regulations on personal information and security detection and evaluation of key information infrastructure.This determines that data security protection should be "data-centric", establish a security protection and governance system, focus on data and ecology, clarify the use, storage and transmission scenarios of data, and build a protection and governance system covering the whole life cycle of data, which is composed of data security organization management, compliance governance and technical protection.

4.4 Strengthening the prevention and governance of cyber hacking attack

Hacking attacks are universal, and common means include e-mail attacks, network monitoring, virus implantation and denial of service.The following measures can be taken to prevent it. First, the firewall technology has continuously enhanced the pre-interception function [9]. Firewall is a security gateway established between Internet and Intranet, which protects Intranet from external illegal users.The firewall has a good protection function, and intruders must go through the firewall to contact the target computer. All incoming and outgoing information must pass through the firewall, and the firewall will become a checkpoint of security issues and refuse suspicious access.Second, the intrusion detection system predicts the security of the system in advance [10]. Intrusion detection system can effectively record and monitor the overall state and trajectory of system operation, and once unauthorized operation behavior is found, it will immediately remind the system administrator to pay attention to and deal with it.Third, network vulnerability scanning can find security problems at any time. Hackers always find the intrusion point in the network by looking for security vulnerabilities, use network scanning software regularly, automatically detect the network security environment, analyze the vulnerability of the network state, and detect the possible vulnerabilities of network equipment by simulating the general steps of hacking.

5. Conclusions

With the development of information technology, the information data generated by human beings has increased rapidly in the form of "data explosion", involving transportation, medical care, industry, biology and finance.At the same time, with the development of storage technology, the cost of data storage is getting lower and lower, and the means of obtaining data are becoming more and more diversified. In the face of the rapid development of information technology in the big dataera, how to effectively protect the security of personal data is particularly important.The wide application of new technologies in the big dataera makes it difficult to divide the network "boundary". The original technical means based on traditional information security protection ideas and focusing on fixed "boundary" attack and defence have been difficult to meet the current needs of personal information protection. The superposition of old and new problems requires new ideas and technical means of information security protection.This paper puts forward personal information security protection measures in the big dataera from many angles, which is of great significance for promoting the application of big data, protecting personal information security and maintaining social stability.

Acknowledgements

This work is supported by Jiangsu innovation and entrepreneurship doctor project: Research on personal information security protection protocol in big data; Natural Science Foundation of Changzhou College of Information Technology (CXZK202004Y): Research on the model and service discovery mechanism for the future distributed social network; Scientific Research and Development Center for Colleges and Universities of the Ministry of Education, China University Innovation and

ISSN 2522-3488 Vol. 7, Issue 2: 59-63, DOI: 10.25236/IJNDES.2023.070210

Research Fund (2021LDA06008): Steel product defect detection based on big data and industrial vision.

References

[1] W. Zhao, M. W. Shui. Research on Personal Information Security Protection Measures under the background of Big data[J]. Computer Programming Skills & Maintenance, 2018, 25(07): 86-87+93.
[2] Pintsotsom. Research on Personal Information Security Protection in the era of Big Data[J]. Wireless Internet Technology, 2022, 19(10): 18-19.
[3] D. F. Zhang. Discuss the significance of protecting personal information security in the era of big data[J]. Electronic Technology & Software Engineering, 2015, 4(22): 208-208.
[4] Y. Dong. Cyber hacker attack and prevention and management in the era of big data[J]. Network Security Technology & Application, 2021, 21(05): 68-70.
[5] G. C. Wang, Z. L. He. Research on Personal Information Security Protection Strategy based on Big Data background[J]. Science and Technology & Innovation, 2022, 8(06): 116-118.
[6] Z. Q. Deng. Analysis of personal information security protection in big data environment[J]. Computer Knowledge and Technology, 2019, 15(03): 33-34.
[7] Y. Liu. Discussion on the legal protection of personal information under the background of big data[J]. Legality Vision, 2022, 38(19): 69-71.
[8] L. P. Zhang, Y. Zhang. Personal Information Security Protection in the context of Big Data: A Study on legal prevention[J]. Modern Business Trade Industry, 2018, 39(16): 126-127.
[9] L. Q. Ming. The trend and countermeasures of cyber hacker crime[J]. Journal of Shandong Police College, 2020, 32(01): 104-113.
[10] G. Q. Xie. Analysis of the common means and prevention of network hacker attacks[J]. Information Technology and Informatization, 2018, 43(05): 129-130.