Research on Personal Information Protection from the Perspective of Enterprises

Jinlan Guo

School of Artificial Intelligence and Law, Shanghai University of Political Science and Law, Shanghai, China

Keywords: Personal information, Enterprises, Information protection

Abstract: With the publishing of regulations on personal information protection in the United States, the United Kingdom, and the European Union, companies that collect, use and controls personal data and companies that provide data security technologies must adapt to this situation, or it will result in huge fines or the danger of exiting market competition. This paper examines how enterprises can evaluate their personal information protection technologies and personal information protection management strategies according to Personal Information Protection Act, in order to comply with the requirements of the law and the public on the protection of personal information and to be invincible in the competition.

1. Introduction

With the development of Internet of Things, big data and cloud computing, and deep learning technologies, the era of artificial intelligence is coming. “Everything is inter-connected, everyone is online, everything is with algorithm”. Algorithms are at the core of artificial intelligence, but without data as raw materials for artificial intelligence, it can do nothing. “Personal data “or “Personal information” in this paper refers to information that can identify the subject. Article 4 of *EU General Data Protection Regulation* (GDPR) adopts a general formulation of the definition of personal data that “Information related to any identified or identifiable natural person (data subject); the identifiable natural person is an individual that can be identified directly or indirectly, especially through such information as name, ID number, location data, online identification, or one or more factors related to the body, physiology, genetic, psychology, economy, culture or social identity” [1]. In China, the term personal information is used for personal data. *The Personal Information Security Regulations of China* (GB / T35273-2017) adopted enumerated expressions for the definition of personal information: Various types of information recorded electronically or in other ways that can identify the identity of a specific natural person or reflect the activity of a specific natural person, alone or in combination with other information, including name, date of birth, identification number, personal biometric information, address, communication contact information, communication records and contents, account password, property information, credit information, whereabouts, accommodation information, health and physiological information, transaction information, etc[2]. It is necessary to point out that the enumerated method does not include private information such as dating situation, hobbies, and even sexual orientation through the user-chain relationship in the social network.

In 2016, Facebook's personal data breach case was suspected of affecting the US election, raising global concerns about the security of personal information on the Internet. On January 21, 2019, the French data supervisory agency also imposed a high fine of 50 million euros on Google for violating the transparency principle of *General Data Protection Regulation*. On February 2, 2019, it was reported that the face recognition software dispute case of Facebook that started in 2015 will cause FACEBOOK to face a fine of 550 million dollars. The cause of it is that Facebook has tested and launched facial recognition software without anyone's consent, users can tag photos with the software, but the test was not approved by its users. While GOOGLE, FACEBOOK and other enterprises have repeatedly issued sky-high price tickets, domestic information companies such as Baidu, Tencent, and Ali are more fortunate, but this is obviously not because these companies have

  DOI: 10.25236/edbm.2020.059

higher awareness of personal information protection than similar companies in the United States. The main reason is that China has always had a looser legal environment for the protection of personal information. However, with the strengthening of international and domestic laws on the protection of personal information, Chinese enterprises, like foreign enterprises, have to seriously face various types of personal information protection compliance issues. Therefore, research on how to develop personal data protection standards, technical standards and evaluation management has theoretical and practical significance.

2. The Current Situation of Related Research in China

In recent years, with artificial intelligence technology going deeper into daily life, legal practitioners and policy makers, consumers have realized the importance of protecting personal information. The *Decision of the Central Committee of the Communist Party of China on Upholding and Improving the Socialist System with Chinese Characteristics, Promoting the Modernization of the National Governance System and Governance Capability* emphasizes that "Promote the construction of digital government, strengthen the orderly sharing of data, and protect personal information in accordance with the law." Under this background, Chinese scholars have gradually increased their research on the protection of personal information in the context of artificial intelligence. In 2019, Xuetao Liu published the article *Challenges and Responses of Personal Data Protection in the Perspective of Administrative Law in China*", pointing out the huge challenges that China's administrative regulations is facing on personal information protection. Zhifeng Zheng published Privacy *Protection in the Age of Artificial Intelligence* in *Science of Law (Journal of Northwest University of Political Science and Law)* in the second issue of 2019. The article deeply analyzed the serious privacy crisis caused by the era of artificial intelligence. In 2015, Wei Yu published *Research on the Legislation of Personal Information Protection under the Background of Cloud Computing* which mainly discussed the current status of China's personal information legislation and explored how to balance the protection and use of personal information. *Research on Criminal Law Protection of Citizens' Personal Information under the Background of Big Data*, written by Yusong Wang, analyzed the necessity of criminal law protection from the current situation of criminal law protection of citizens' personal information, and proposed corresponding solutions to the current dilemma, which provided some reference to perfect the relevant criminal law protection. Weiwei Cai 's *Research on the Criminal Law Protection Strategy of Citizens' Personal Information* suggested that personal information needs to proceed from different levels and improve the legal protection of citizens' personal information security. In summary, these scholars have fully analyzed the inadequacy of the laws about personal information protection, as well as the issue of law enforcement and the relief for personal information violations.

However, at the moment when new personal information protection laws have been introduced or are being introduced, there has not been any research to analyze how enterprises build a system that values personal information protection internally, establish standards that meet future personal information protection technologies, and establish internal personal information protection management System and evaluation system. Especially for Chinese domestic enterprises, under the domestic loose personal information legal environment, some companies do not pay attention to the protection of personal information. If this style is not changed, it may not be able to adapt to future market competition.

3. Inevitability for China to Bid Farewell to the Loose Environment of Personal Information Protection, and Certainty to Strengthen Personal Information Protection

Yanhong Li, the CEO of Baidu, once said that Chinese people are not so sensitive about privacy issues, and they are willing to trade privacy for convenience. Although what he said caused criticism, it reflected that the Chinese people's awareness of privacy protection is not strong, and the government's personal information protection laws have always lagged behind in this regard.

Judging from the incidence of crimes against personal information of citizens in China, there were almost no cases between 2009 and 2012, and such crimes rarely occurred in judicial practice; The number of cases gradually increased from 2012 to 2016, but the total number of crimes was small, and the crime was low-price running; The number of cases increased by 214.6% from 2016 to 2017, the rate of increase was extremely fast, and crime showed a high incidence. Yuyu Xu, a prospective college student in 2016, was the victim of personal information leakage. Telecommunication fraud caused property damage and psychological stress to this girl who was born in a poor family. Her death caused great indignation among the people across the country. In 2017, a CCTV reporter found that on the black market, information such as the phone call history, trip history, QQ chat history can all be listed as long as there's a mobile phone number. These personal information incidents will prompt the government to resolve the problem of personal information leakage.

The voice of netizens on the protection of personal information is growing. In *China Internet Association's Survey Report on the Protection of the Rights and Interests of Chinese Netizens 2016*, 54% of netizens thought that the leakage of personal information was serious, and 21% of them considered it very serious. 84% of netizens have personally felt the adverse effects caused by the leakage of personal information. The 44th *Statistical Report on Internet Development in China* in 2019 stated that the netizens reached 854 million and the Internet penetration rate reached 61.2%. Personal information leakage in 2019 has become the highest proportion of network security issues, reaching 24.0% (Figure 1). It has become the primary problem that netizens suffer from various network security problems [3].

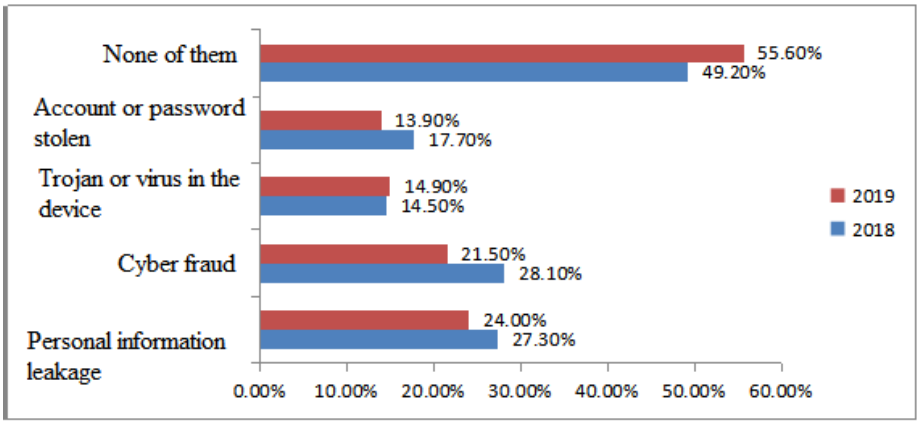

Fig.1 Various Cybersecurity Issues Netizens Suffer

On January 24, 2018, *Personal Information Security Regulations of Information Security Technology* was officially released. It covers the aspects such as collection, storage, use, sharing and transfer of personal information, and security incidents handling. New revisions were made in October after seeking for opinions in 2019. Although it is only a recommendation standard, the overall requirements in terms of content are no less than international standards. For example, it requires organizations to carry out personal information security training, and it stipulates the principle of personal information protection, the organizations' size of the personal information protection and the personal information processing quantity; It requires the establishment of a personal information security impact assessment system and regular (at least annually) a personal information security impact assessment; It requires background checks on insiders who have access to personally sensitive information, requires assessment in addition to training; It also uses automated audit tools and requests a personal information security audit.

4. How Can Enterprises and Institutions Improve Their Personal Information Protection Capabilities to Adapt to the New Market Environment

From the public news, BGI (The Beijing Genomics Institute) was held accountable by the Ministry of Science and Technology for the impact of the leakage of DNA samples from 140,000

pregnant Chinese women. To be practical, these continuous outbreaks of personal information leaks are caused by less protection of personal information by enterprises. When the enterprise developed a new product, as long as it met the functional and performance requirements, the product could be applied and promoted to the market at one time. When China issued *Personal Information Security Regulations*, enterprises have a reference standard: What is the scope of personal sensitive information; How is this sensitive information stored, processed, and used; How does the software involving sensitive information be managed in operations. In the long run, enterprises must implement strict personal information protection policies in order to gain users' trust in the future in order to develop the enterprises' business.

4.1 Strengthening Corporate Responsibility and Pursuing the Three Principles of Personal User Information Protection

When people participate in economic activities, they often need to register accounts and fill out forms. In this process, enterprises should ask for users' consent, inform them of the purpose and scope of personal information, and fulfill the responsibility of security protection. In January 2019, the four departments including Office of the Central Cyberspace Affair Commission, Ministry of Industry and Information Technology of People's Republic of China, the Ministry of Public Security of People's Republic of China, and State General Administration of Market Regulation jointly issued the *Announcement on the Special Administration of the Collection and Use of Personal Information by APP Illegally*, which explicitly prohibited the above-mentioned illegal operation. People who collects are responsible. It required that the user's knowledge and consent be obtained in advance for information collection.

Based on China's current laws on the protection of personal information, enterprises need to implement three principles in the protection of personal information: the principle of notification and selection, the principle of minimum necessity, and the principle of risk assessment. The principle of notification and selection means that users have the right to be notified when the personal information is collected by the enterprise. Users have the right to decide whether the enterprise can collect their personal information on the premise of knowing the facts. The connotation of the minimum necessary principle includes two aspects: First, the personal information collected must be directly related to the realization of the product or business function; Second, the frequency of automatic collection of personal information must be the minimum required frequency, and the amount of information obtained indirectly should be the minimum required. Risk assessment refers to the fact that an enterprise collecting information can evaluate the risks that the information may bring and provide a response plan, so that it can formulate a corresponding personal information protection policy more accurately.

4.2 Strengthen Corporate Responsibility and Protect users' Personal Information When Working with Third Parties

In the current situation, the balance of responsibility for the protection of personal information has been biased towards enterprises. The 44th *Statistical Report on Internet Development in China* in 2019 stated that As of June 2019, netizens in China have reached 854 million. Most of them focus on instant messaging such as WeChat and QQ, search, shopping and social platforms. The netizen utilization rate of instant messaging was 96.5%, that of search engines was 81.3%, that of online news users was 80.3%, that of online videos was 88.5%, and that of online shopping was 74.8%.The number of mobile apps per capita of netizens aged 15-19 reached 66; the number of mobile apps per capita of netizens aged 20-29 was 54; the number of mobile apps per capita of netizens decreased with the increase of age. Among them, the number of mobile apps per capita of netizens aged over 60 was 33[3].

When netizens use these social platforms and APP applications, they must log in, register. When being provided services, they are often asked to offer their information, such as mobile phone numbers, ID numbers, address books, location information, and address information. If the information between the two commercial organizations starts to exchange and merge, thet can realize the real-time tracking and monitoring of personal online and offline behavior through the

comparison and cross-validation of personal information from multiple sources. People will have nowhere to hide [4].

First, when cooperating with other organizations, enterprises should first clarify the relevant provisions in the Consumer Rights Protection Law: The operator and the staff must keep the personal information of consumers collected strictly confidential, and must not disclose, sell or illegally provide it to others. Secondly, *Personal Information Security Regulations* stipulates that if automation tools (such as code, scripts, interfaces, algorithm models, software development kits, applets, etc.) embedded or accessed by third parties are involved, technical testing should be conducted to ensure that the collection and use of their personal information meet the regulations. It also regulates that the behavior of collecting personal information by automated tools embedded or accessed by third parties should be audited. If any behavior is exceeded, the access will be cut off in time. At present, many enterprises and institutions, especially financial, operator, medical, social security, education, and government agencies that are closely related to the collection and use of personal information, have a large amount of customer data. They use data mining and artificial intelligence technology to develop business needs, but they do not have IT technology capabilities. As a result, they have more ways of doing business with third parties. These enterprises must carefully study the standard and carry out related data security construction activities, not only adopting corresponding data protection technologies, but also auditing the qualifications of third-party cooperation agencies. They also need to prevent the behavior of mining users' true identities from anonymized and obfuscated data through technical means. When information leakage or loss occurs, remedial measures should be taken immediately [5].

4.3 Improving Privacy Protection Technologies to Protect the Personal Information of Citizens

Privacy protection technology includes the protection of user information in three aspects: storage, search, and computing. If the cloud server that stores a company's big data is owned by the company, the computing privacy issue of the data will be automatically eliminated. If it is not its own cloud, it must choose a company that meets the legal requirements for the protection of personal information. Current data encryption technologies are capable of these three tasks. For example, a fully homomorphic encryption scheme can achieve the security of data protection, search, and computing, but it will affect operational efficiency. It seems that on one hand, data security experts need to design fully homomorphic encryption algorithms that run more efficiently. On the other hand, people must sacrifice some data query and calculation efficiency to ensure their privacy [6].

4.4 Standardize enterprise management, improve the internal management system and confidentiality system of the enterprise, divert key authority, and prevent internal staff from stealing information by using their authority

Enterprises need to strengthen employees' information security education, conduct personal information security training, so as to increase their awareness of security precautions and legal awareness, and prevent information leakage due to work errors [2]. Enterprises need to conduct background checks on internal personnel who have access to personal sensitive information. In addition to training, they also need to assess and use automated audit tools and carry out personal information security audit [2].

Relevant departments need to pick a person in charge of personal information protection and set up a personal information protection agency. The size of the organization and the amount of personal information processed can be found in *Personal Information Security Regulations*.

Personal information security impact assessment system needs to be established, and be conducted at least once a year [2].

5. Conclusion

Enterprises should strengthen internal management regulations to protect personal information security in accordance with relevant laws and regulations such as *Consumer Rights Law* and

Personal Information Security Regulations. However, the protection of personal information is about everyone. The government, society, enterprises and individuals should work together to better protect personal information, so that people's work and life will be more assured and more secure.

References

[1] Chunhui Wang. Comparison of GDPR Personal Data Rights and Personal Information Rights under Cybersecurity Law [J]. China Information Security. 103(7):40-43(2018).

[2] National Information Security Standardization Technical Committee. Information Security Technology Personal Information Security Regulations issued by Standardization Administration of People's Republic of China [EB / OL]. 12.29(2017).

[3] China *Internet* Network Information Center (CNNIC). The 44th Statistical Report on Internet Development in China.

[4] Bin Wang, Kangqing Wang. Actuality of Crimes Against the Personal Information of Citizens and Countermeasures [J]. Journal of Guangxi Police College. 32(2019).

[5] Xuetao Liu. Challenges and Responses of Personal Data Protection from the Perspective of Administrative Law in China [J]. Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition). 2(2019).

[6] Liusheng Huang, Miaomiao Tian, He Huang. Review of Big Data Privacy Protection Password Technology. CNKI Web-first publishing. 02.02(2015).