Personal Information Data Security Prevention and Control From the Perspective of Corporate Criminal Compliance

Xiaofan Bi[1]

[1] *School of Law, Humanities and Sociology, Wuhan University of Technology, Wuhan, Hubei, China*

ABSTRACT

In the digital age, data is undoubtedly the core asset of an enterprise. The rational use and processing of personal information data can allow enterprises to enjoy the convenience and intelligence brought by digital progress. However, with the pains of the data era, the simple infringement of personal information has gradually evolved into harming personal data, commercial data, public data, and national data, which has led to data security issues. In practice, laws to protect data and information such as the Personal Information Protection Law, the Data Security Law, and the Cybersecurity Law have been promulgated, but these are more post-event liability regulations for infringing data and information. This article will put forward prevention and control suggestions from the perspective of encouraging corporate criminal compliance, regulatory effectiveness criminal compliance, and the establishment of a criminal compliance system by the company itself.

Keywords: *Personal information, Data security, Criminal compliance, Enterprise risk prevention and control.*

1. INTRODUCTION

Since the birth of the Metaverse, data has become an indispensable element, and personal information data is undoubtedly an important part of such data [1]. Faced with the challenges and alienation of data security such as corporate personal information in the context of the metaverse, people only rely on the normative clauses in the Criminal Law, the Personal Information Protection Law and the Data Security Law to conduct post-mortem actions against personal information and data violations. This is inevitably lagging, limiting, and passive. Corporate criminal compliance generally refers to state-owned enterprises and private enterprises, in order to prevent the criminal risks of the enterprise itself and its executives, through professionals to diagnose the criminal risks of the enterprise from life to death, so as to implement prevention and control measures to prevent possible existence in the process of enterprise operation. To reduce or prevent the criminal risk that has already occurred, so as to "treat the disease before the disease, and treat the disease that you want to treat." An effective and reasonable criminal compliance program can open up new frontiers for entrepreneurs and escort the longevity of enterprises. A reasonable and effective criminal compliance program can open up new frontiers for entrepreneurs and escort the longevity of enterprises. The criminalization of corporate compliance has recently become a hot topic of the rule of law for various enterprises. It is a significant sign of the transition of the state's governance of corporate crimes from "light prevention and heavy punishment" to "prevention first and both punishment and prevention". It is related to the healthy development of business operations.

2. INFORMATION WAR: THE BACKGROUND OF ENTERPRISE PERSONAL INFORMATION DATA RISK PREVENTION AND CONTROL

With the rapid development of new technologies such as computers, incidents of

infringing on citizens' personal information frequently occur, and the leakage of citizens' personal information and data has become the focus of current society. Based on the development status and future trends of crimes against personal information, this paper explores the leakage of personal information from the perspective of corporate criminal compliance.

2.1 Current Status of Crimes Against Personal Information

In the context of today's information age, personal information is no longer just a representation of personal interests, but also reflects huge property interests. In practice, there are countless profit-making behaviors by companies infringing on personal information, which has seriously affected people's life. Since the beginning of the 20th century in my country, people have entered the era of electronic information, and the communication method is no longer limited to face-to-face conversations, but also communicates information through Weibo, WeChat, QQ, and email. When people use electronic products, they need to enter their personal information such as their name, gender, mobile phone number, ID number, address, etc. from time to time to obtain access to the Internet. They provide their personal information to the outside world almost every day. Many people do not know their own personal information. Information and data security is facing great hidden dangers, or even if you know that your personal information is being violated, you will be immersed in it for the purpose of surfing the Internet. Some criminals have become rampant, wantonly infringing on citizens' personal information and data. [2]

2.2 Risks of Infringing Personal Information and Data in Enterprises

On May 22, 2022, the author visited China Judgment Documents Network. After screening the three conditions of "criminal case", "criminal cause of action", and "unit crime", and roughly browsed the themes of these cases, among them, companies violated personal information. There are not many cases, but compared with 2015, the frequency of corporate crimes has increased, which to a certain extent indicates that the number of personal information risk crimes in Chinese enterprises has increased year by year with the convenience of Internet technology and big data applications. fast trend characteristics. In actual market activities, the network facilities and information data operated and managed by various units are concentrated in large quantities, whether it is "passive leakage" caused by poor management or "active leakage" by illegal personnel of the unit, once it is damaged or data is leaked, it must seriously endanger personal information security. If these enterprises are national infrastructure enterprises, such as government agencies, education, national defense, TV stations, etc., information leakage will even affect the national economy, people's livelihood and public interests.[3]

With the increase in the value of citizens' personal information, the leakage of personal information in some units is not a new case. In recent years, the case of "Zhilian Hiring" employees participating in reselling citizens' information has alarmed the whole network [4]. However, according to Jianzhuo Xu, the head of the Internet Technology Research Center of the Ministry of Public Security, the major hazards to public information disclosure are banking, education, telecommunications, express delivery, securities, e-commerce and other service industries. With a large amount of information, corporate insiders are also more likely to leak personal data. According to the "Annual Report on Personal Information Protection" issued by the Nandu Cyber Security Research Center, the platform ignores the serious problem of users' personal information, and Zhilian, Liepin, and Ganji in the recruitment platform are ranked at the bottom. In this case, Zhilian's internal employees took advantage of management loopholes to resell personal information without permission. Since Zhilian failed to fulfill its corresponding security obligations, it needs to bear civil compensation liability for customers whose personal information was leaked. In practice, in the face of the leakage, damage and loss of personal information that has occurred or will occur, only a few companies can take remedial measures such as initiating emergency measures, informing users who have suffered losses in a timely manner, and reporting to relevant local government authorities.

3. THE ROAD MUST BE: A REALISTIC FOUNDATION FOR CORPORATE CRIMINAL COMPLIANCE PROGRAMS

Enterprises exist as profit-making organizations, and costs and benefits are always the core of their concerns. In the process of pursuing profits, general

illegal costs (such as involving civil liability and administrative liability) are acceptable to enterprises, but only criminal liability is the responsibility of enterprises. The last red line is not too much a "disaster" for entrepreneurs. Therefore, enterprises should establish a criminal compliance system, diagnose the criminal risks existing in the enterprise (including the enterprise itself and its executives), and propose prevention and control suggestions and plans.

3.1 The Necessity of Criminal Compliance of Enterprise Personal Information Data Prevention and Control From Cases

The "Nestle case" in 2017 is a typical example of a company implementing a personal information compliance mechanism to avoid the risk of corporate "unit crime". On October 31, 2016, Chengguan District, Lanzhou City Court of First Instance convicted and punished the crime of infringing citizens' personal information for the behavior of Mr. Zheng and other employees of Nestlé China who obtained information such as names and mobile phone numbers of pregnant women by paying facilitation fees. Subsequently, Zheng and others appealed and argued that their actions were not personal actions and should be corporate actions. On May 31, 2017, the Lanzhou Intermediate People's Court made a final judgment of the second instance, upholding the original judgment. The main text of the judgment of the court of second instance used "Nestlés policies, employee code of conduct and other evidence to prove that Nestlé prohibits employees from engaging in illegal and criminal acts that infringe on citizens' personal information, and that the appellants violated the company's management regulations and committed crimes in order to improve personal performance." It was determined that the criminal acts of Zheng and others were personal acts and non-unit acts, so Nestlé was not identified as a unit crime. [5]

In the above-mentioned cases, Nestlé used its effective compliance mechanism to separate the corporate responsibility from the employee's personal responsibility, and cited corporate compliance as a sufficient basis for its innocence defense, thus successfully avoiding the corporate responsibility. Criminal liability prevents enterprises from falling into the disadvantageous state of unit crime. This case can prove that an effective compliance mechanism has great practical significance for enterprises to prevent and reduce the risk of unit crime [6].

3.2 The Legitimacy of the Criminal Compliance of Enterprise Personal Information Data Prevention and Control

In modern society, the complexity of operation and management and the strictness of the criminal law network for market economic activities have increased the risk of violation of the law for small and medium-sized enterprises. Therefore, the establishment of criminal compliance management to prevent future risks has become a new trend in enterprise development. Compliance, as the name suggests, is compliance with the requirements of the specification. In the United States, the compliance program is considered to be an "internal mechanism for detecting and preventing internal crimes" [7].

Criminal compliance plays an escort role in the operation of enterprises in economic and social life [8]: First, optimize the company's internal structure. As long as a company establishes an effective compliance plan, it will bring new changes to the company's governance structure. The company's compliance department will conduct internal independent reviews in various business operations, financial supervision, and even talent management. Second, increase insurable benefits. In the short term, some companies may increase their interests by adopting illegal means in their business activities, but such interests are not guaranteed, because improper means will damage the company's reputation and undermine the company's long-term interests. Through the establishment of an effective criminal compliance plan, enterprises can obtain longer-term and overall protection of interests by carrying out business activities under the premise of legal compliance. Finally, prevent crime from happening. The purpose of introducing criminal compliance is to avoid criminal liability for the company or its employees. Once convicted and sentenced, it will cause heavy losses and pay a heavy price. Therefore, only by establishing an effective compliance plan can an enterprise better restrain itself, operate with integrity, establish a good social image, gain a long-term business reputation, and achieve sustainable and healthy development.

4. PLAN AHEAD: THE PERFECT PATH FOR CORPORATE PERSONAL INFORMATION DATA CRIMINAL COMPLIANCE

In the face of the diversity and complexity of corporate personal information crime risks, it is of great significance to build a corporate compliance plan, but it is not easy to establish a complete criminal compliance plan and ensure its effective implementation.

4.1 Local Exploration of Corporate Personal Information Data Criminal Compliance

The "Personal Information Protection Law" is China's first separate legislation on personal information protection, opening a new chapter in the legal cause of personal information protection in China. From the perspective of "Personal Information Protection Law"[9], the data compliance risks faced by various enterprises can be said to cover all aspects of business operations. Under the framework of the Personal Information Protection Law, whether it is the institutional system including user agreements, privacy policies, etc., upstream and downstream enterprise management, product quality, business overseas, or information disclosure, marketing, intellectual property and other aspects of enterprise operations, there are hidden data compliance risks. Among them, the most common types of personal information infringements are excessive collection of user information, illegal use of user information, big data killing, illegal "selling" of personal information, excessive use of face recognition information, and cross-border data. The best way to root out the illegal and infringing use of personal information and protect the security of personal information is to establish a data compliance system within the enterprise "from the inside out", and formulate internal management systems and operating procedures, which is also stipulated in the "Personal Information Protection Law".

"Cybersecurity Law" [10], in recent years, has been fully implemented. At the same time, the "two highs" have issued a special judicial interpretation on the crime of infringing on citizens' personal information, "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing Citizens' Personal Information" (hereinafter referred to as the "Interpretation"), which constitutes the "Internet The important mechanism supporting the Security Law. Judging from the relevant content of the "Cybersecurity Law", as the main subject of personal information, enterprises are also participants of online platforms, and they are bound to assume important subject responsibilities. At the same time, under the guidance of the Interpretation, criminal issues related to personal information are more targeted. For example, Article 3 of the Interpretation specifies "citizens' personal information", and Article 4 specifies "other methods for illegally obtaining citizens' personal information" [11]. The content of the "Interpretation" will help various enterprises to further design business compliance strategies for behaviors related to citizens' personal information on the basis of the general system requirements of the "Cybersecurity Law", and also help various enterprises to build a criminal risk prevention framework For example, Article 7 of the Interpretation clearly stipulates the application of penalties for unit crimes, and Article 10 clearly stipulates the reasons for exemption. With these two interpretations as the normative guidance, various types of unit subjects can better establish a blocking mechanism, so as to achieve the purpose of reducing or even eliminating their own subject liability under legitimate circumstances. In short, under the guidance of the normative system of the Cybersecurity Law and the Interpretation, all types of enterprises should improve their risk control capabilities, form risk control norms for business management and development, reduce the possibility of triggering criminal acts, and achieve The Benign and Effective Self-discipline and Management of Organizations [12].

In the era of digital economy, data has become a new factor of production. China's various industries are rich in data resources, and stakeholders are competing fiercely for data resources, and data security issues are becoming increasingly prominent. The promulgation of the "Data Security Law" regulates data processing activities, ensures data security, and promotes data development and utilization. The digital economy involves the roles and responsibilities of users, merchants, platforms, third-party service agencies and other subjects in the data industry chain. A healthy digital economic order needs to correctly deal with the balance between data property protection, data security and personal information, forming Reasonable data security governance system. Article 4 of the "Data Security Law" stipulates: "To maintain data security, it is necessary to adhere to the overall

national security concept, establish and improve a data security governance system, and improve data security assurance capabilities." This puts forward more detailed measures for enterprises' data criminal compliance construction. Data criminal compliance is a new content of the modern enterprise governance system in the era of big data, emphasizing that enterprises should actively prevent data criminal security risks with their own efforts and eliminate data-related crimes in the bud.

"Data Security Law" [13] regulates data processing activities from the aspects of supervision system, data security and development, data security system, data security protection obligations, government data security and opening, legal responsibility, etc., effectively supplementing the Cybersecurity Law, Personal Information Protection deficiencies of the Act in regulating data processing activities. The "Data Security Law" will, together with the "Network Security Law" and the "Personal Information Protection Law", comprehensively build a legal framework for China's data security field. In the future, data disputes between enterprises will be governed by laws, and legality and compliance will become a new threshold for enterprises to operate data services.

4.2 Improvement Measures for Criminal Compliance of Corporate Personal Information Data

First, businesses are encouraged to establish and maintain personal information criminal compliance programs. For example: Criminal sanctions can be reduced if the company can demonstrate that it has an effective compliance system, which is a solution implemented in the context of Chinese criminal law sentencing standards. People can observe that due diligence is becoming more and more popular in discussions about the best way to clarify corporate criminal liability. The goal of both hypothetical approaches to corporate criminal compliance is to protect against corporate personal information risk. Through criminal compliance, the state essentially aims to use the company's own interests to manage legal risk, and by providing the right incentives, the company's risk management function ultimately has a preventive effect in the public interest.

Second, the compliance department should conduct a substantive review of the effectiveness and rationality of the company's compliance program. In theory, it is easier for an enterprise to demonstrate an effective solution after sufficient due diligence. However, in practice, there is a must to admit that the compliance effectiveness of an enterprise in preventing and detecting personal information crimes is difficult to manage and measure. Empirical research shows that compliance programs can have a positive impact on the behavior of those who work for a company, but only if formal compliance measures are supported by the generality of the company. Therefore, corporate compliance departments should tend to focus on establishing and maintaining demonstrable measures.

Finally, there is a must to grasp the three key points of the corporate personal information criminal compliance system. The three key points mean "people, money, behavior". Persons refer to corporate executives and ordinary employees. Through the compliance management of executives and employees, individual behaviors and corporate behaviors can be clarified, so as to prevent employees' personal behaviors from causing crimes by corporate units. Money refers to the management of funds. The crime of embezzlement and misappropriation of funds are high-frequency crimes related to money. Behavior refers to an enterprise's own code of conduct, access to qualifications, business development and new additions, listing and financing, external transactions, internal labor and personnel management and other aspects of corporate behavior. Criminal compliance proceeds from these three lines. To establish a targeted criminal compliance system, for example, to establish a personal information protection system, it should be based on the Cybersecurity Law and the Personal Information Protection Law, combined with the crime-related norms in the Criminal Law, and on the basis of analyzing the composition of the crime.

5. CONCLUSION

In the era of digital economy, the traditional personal data security crisis and the new type of data crisis overlap and overlap, resulting in many problems. China's current personal information crisis early warning system is still flawed, and an effective criminal compliance mechanism is urgently needed to improve it. At the same time, in the current legal market, the growth of the company must not grow savagely on the track of profit-seeking, and it needs a strong backing to escort the company. Criminal compliance has well undertaken this task, an effective criminal compliance program has many advantages for a business: for example,

optimizing the company's internal structure, increasing secure benefits, and preventing crime. However, this road is also a long way to go. In the increasingly complex international environment, only by continuously improving their own criminal compliance system to gain more competitive advantages can domestic enterprises give enterprises a clean and bright future for development.

AUTHORS' CONTRIBUTIONS

This paper is independently completed by Xiaofan Bi.

REFERENCES

[1] Wang Defu. New Challenges and Legal Responses to Personal Information Protection in the Metaverse Field[J]. China Market Supervision Research, 2021(11):60-62, p.60. (in Chinese)

[2] The Status Quo and Development Trend of Crimes Infringing Citizens' Personal Information in my country [J]. China Anti-Counterfeiting Report, 2020(6):60, p.60.(in Chinese)

[3] Wang Hao. Research on the Prevention and Control System of Citizens' Personal Information Security [J]. Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition), 2020, 41(12): 82-87, pp. 83-85.(in Chinese)

[4] Li Fangling, Yang Jian. Employment Analysis of Library and Information Major Students Based on Employers [J]. Inner Mongolia Science and Technology and Economy, 2020(17):52-54, Page 53. (in Chinese)

[5] Li Si. Analysis of Nestl ê s cross-border M&A experience and its enlightenment to Chinese enterprises [D]. Beijing: Capital University of Economics and Business, 2014, p.3. (in Chinese)

[6] Liu Wei. Traceability, Reflection and Construction of Criminal Compliance [J]. Jianghai Academic Journal, 2021(4):173-180, p.176.(in Chinese)

[7] Wang Zhigang, Qin Ji. On the Substantive Effectiveness of Criminal Compliance Programs [J]. Journal of Southwest Petroleum University (Social Science), 2022, 24(1):75-85, pp. 76-77.(in Chinese)

[8] Li Xiaolong. Criminal Compliance of Internet Finance in the Digital Age [J]. Journal of Nanjing University (Philosophy. Humanities. Social Sciences), 2021,58(5): 97-111, pp. 99-106.(in Chinese)

[9] Peng Kun. On the cross-border flow system of personal information handled by state organs — taking Article 36 of the "Personal Information Protection Law" as the entry point [J]. Journal of East China University of Political Science and Law, 2022, 25(1): 32-49, pp. 33-48.(in Chinese)

[10] Guo Chunzhen, Zhang Hui. Research on State Capability in my country's Cybersecurity Rule of Law [J]. Jianghai Journal, 2021(1):163-170, pp. 164-167.(in Chinese)

[11] Ye Liangfang. The proper interpretation of "violation of relevant state regulations" from the perspective of the unity of legal order: Commentary on Article 2 of "Interpretation on Several Issues concerning the Application of Law in Handling Criminal Cases of Infringing Citizens' Personal Information" [J]. Zhejiang Social Sciences, 2017 (10): 15-23, pp. 16-20.(in Chinese)

[12] Wang Chunhui. Criminal Legal Liability for Infringing Citizens' Personal Information-Analysis of "Two Highs" Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing Citizens' Personal Information [J]. People's Rule of Law, 2017 (9):10-13, pp. 12-13.(in Chinese)

[13] Zhang Yan. Research on the Construction of the Rule of Law in Data Security [J]. Cooperative Economy and Technology, 2021(17):184-185, p.184. (in Chinese)