Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030106
ISSN 2616-2296 Vol. 3 Num. 1

Criminal Legal Risks in Corporate Data Compliance and Suggestions for Prevention

Xindan Huang

Law School / School of Intellectual Property, Guilin University of Electronic Technology, No. 1 Jinji Road, Guilin, Guangxi, China
vision_dy@qq.com

Keywords: Data compliance, Corporate compliance, Criminal law, Risk prevention

Abstract: The application of big data facilitates every aspect of our lives, so many enterprises are willing to use illegal means to obtain more data and snoop on user's data with excessive privileges. However, the illegal collection, application and storage of data not only make enterprises face huge fines and shut down their business, but also may incur prison sentences. How to deal with data within the red line of the law and prevent possible criminal legal risks has become a problem that enterprises should solve nowadays. Enterprises should take the current laws and regulations as the basis, standardize the collection, storage, use and transmission of data to avoid possible criminal risks, establish a data compliance management team, and realize the sustainable development of enterprises.

1. Concepts Related to Enterprise Data Compliance

1.1. Data

In the Data Security Law, data refers to any record of information by electronic or other means; in the Network Security Law, network data refers to all kinds of electronic data collected, stored, transmitted, processed and generated through the network, both of which are broadly defined. While in some individual legislation, a narrow definition is adopted, for example, Article 2 of the Measures for Regulatory Data Security Management of the China Banking and Insurance Regulatory Commission (Trial), regulatory data refers to all kinds of information collected by the CBIRC in the process of fulfilling its regulatory duties, or recognized by the business departments of the CBIRC. After comprehensive consideration, this paper chooses to take the definition in the Data Security Law as the standard.

1.2. Enterprise Data Compliance

The so-called corporate compliance is a set of corporate governance system established by an enterprise to effectively prevent, identify and respond to possible compliance risks. [1]Corporate data compliance belongs to the branch of corporate compliance, which focuses on avoiding risks arising from the processing of data. According to the different behaviors of handling data, it can be divided into different types such as data storage compliance, data exit compliance, data flow compliance, data security assessment compliance, data portability compliance, data crawling behavior compliance, data compliance in special industries, and so on.

1.3. Laws and Regulations Applicable to Enterprise Data Compliance

According to data from the United Nations Conference on Trade and Development, more than 100 countries have enacted data security protection legislation globally, and more than 40 countries have introduced corresponding drafts. [2]The EU adopted the General Data Protection Regulation in 2016, Japan enacted the Personal Information Protection Law Amendment Act in 2020, and Canada introduced the Digital Charter Implementation Act in 2020. The succession of new regulations marks the emergence of data compliance as a high-profile compliance risk area around the world.

China promulgated and implemented the Cybersecurity Law of the People's Republic of China in 2017, and successively promulgated and implemented the Data Security Law and the Personal Information Protection Law, and the judiciary issued the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens' Personal Information, and the Provisions of the Supreme People's Court on the Trial of Nine Cases of Infringing on the Rights and Interests of the Person by Using the Information Network Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Nine Civil Cases of Infringement of Personal Rights and Interests by the Use of Information Networks" to protect personal information.

It can be seen that China's legislation to actively adapt to the wave of the times, the increasingly important data security in the legal scope of protection, China's data security legislation has also entered a period of rapid development, China has officially opened the era of the rule of law in the application and governance of data, the above laws and regulations have also become a basic code of data compliance construction of the current enterprise.

2. Possible criminal legal risks for businesses

2.1 Criminal risks associated with access to information behaviors

Enterprises are suspected of committing the crime of infringing on citizens' personal information if they have illegally obtained citizens' personal information. For example, in the case of "Li, Zhang suspected of infringement of citizens' personal information", the defendant, as a shareholder of a company, before leaving the company, copied the relevant customer information to a USB flash drive and used it for the company's customer marketing, which constituted the crime of infringing on citizens' personal information without the authorization of the subject of the information protection and was sentenced in accordance with the law to the crime of infringing on citizens' personal information.[3]

A company that obtains citizens' personal information by illegally accessing the information system of a government or medical institution is suspected of committing the crime of illegally obtaining computer information system data. In China first data compliance case - The Case of Z Network Technology Co., Ltd, Chen and Others Illegally Obtaining Computer Information System Data - the defendants, using data crawler technology without authorization and permission, instructing a number of technicians to illegally obtain data from a food delivery platform, causing over 40000 yuan direct economic loss, was identified as the crime of illegally obtaining computer information system data.[4]

Enterprises are suspected of committing the offense of infringing upon trade secrets if they are acquiring secret information, etc., of the relevant industry.

2.2 Criminal risks associated with the act of processing information

If an enterprise violates its data security protection obligations and refuses to make corrections or causes serious consequences such as the leakage of large amounts of data, it is suspected of constituting the crime of refusing to fulfill its information network security management obligations. For example, in the case handled by Shanghai Pudong New District People's Court, the defendant, Hu, rented domestic and foreign servers for illegal profit, produced and rented out the *Tushengsun* and *Forty-two* wall-flipping software on his own, and illegally provided overseas Internet access services for more than 2,000 network users in the country. In March and June 2016, Shanghai Municipal Public Security Bureau interviewed defendant Hu twice, and asked him to stop the network service. In October of the same year, the Public Security Bureau imposed administrative penalties on the Defendant in the form of an order to stop networking, a warning, a fine and confiscation of the illegal income. Defendant Hu refused to rectify the situation and continued to rent out the *Tushengsun* wall-flipping software, earning a total of RMB 236,167 in illegal income.[5]The court finally ruled that the defendant had committed the crime of refusing to fulfill the obligation of information network security management, and sentenced him to six months' imprisonment, six months' probation, and a fine of 30,000 yuan.

3. Recommendations for the prevention of criminal law risks

3.1. Establishment of a dedicated compliance management department and data compliance team

The vast majority of multinational enterprises have set up the position of corporate data compliance officer or data protection officer at the request of the countries in which they operate, and 360 is the first large-scale Internet enterprise to set up a chief privacy officer in China.[6] Some companies have also embedded their compliance functions in their legal departments, but there are many differences between corporate compliance and legal work.

Legal work mainly involves legal risks in enterprise business activities, such as breach of contract liability arising from the performance of contracts, labor disputes with employees, etc., so its code of practice mainly refers to laws and regulations. In addition to legal risks in corporate compliance, it is also necessary to deal with social responsibility risks arising from the violation of ethical norms, such as the loss of credibility of the enterprise, so it is also necessary to master the industry guidelines, ethical norms and so on. Work content in addition to managing data protection work, but also with regulatory authorities, data subjects to docking, always grasp the regulatory direction of data compliance.

In addition, specific enterprises should also set up professional data compliance teams in order to meet the management requirements of data compliance. Because electronic data collection, storage, use, etc. is usually specialized, for example, the Shanghai Putuo District Procuratorate publicized the country's first case of criminal compliance in the field of data does not prosecute the case involves the illegal use of network crawlers, so the professional data compliance team should also be equipped with professional computer personnel to assist in the day-to-day work, in order to ensure that professional and neutral compliance personnel to participate in the development and implementation of the criminal compliance program, and to clearly delineate the data compliance management requirements of the enterprise managers. Clearly delineating the compliance responsibilities of enterprise management personnel, ensuring the criminal compliance plan is not just shown on the paper, but implemented in actual work.[7]

To summarize, the iron must be hardened by itself. In order to prevent criminal legal risks, enterprises must first look for breakthroughs from themselves, fill the loopholes within the enterprise, and form a work system that meets the requirements of laws and regulations.

3.2. Establishment of a data compliance management system for long-term operation

3.2.1. Hierarchical categorization of existing data in the enterprise

With reference to the relevant provisions of the Data Security Law, data is categorized into general data, important data, core data, personal information, commercial secrets, etc., matching different governance systems for different levels, reasonably allocating internal resources of the enterprise, and forming a compliance management system.

3.2.2. Identify different hierarchical management systems and develop a categorized governance system

Corresponding compliance management measures have been formulated for specialized data classified in accordance with the aforementioned classification, and different hierarchical management systems have been established to form a categorized governance system. For example, measures such as backup and encryption should be taken for important data, attention should be paid to strictly restricting cross-border transmission of data related to national security, and personal information that needs to be made available outside the country should be subject to strict legal procedures, security assessments organized by the national Internet information department, and protection and certification by professional institutions.

3.2.3. Review every aspect of data processing in its entirety

Data processing includes data collection, storage and cross-border transmission, use and processing, provision and disclosure, and deletion of links. When processing data, enterprises should review each link and assess the level of risk; problems found in any link should be rectified in a timely manner; and the obligation to delete data collected in violation of the law should be fulfilled in a timely manner to avoid compliance risks.

3.2.4. Reasonable allocation of internal resources to form a compliance management system

Enterprises can start from the three dimensions of data categorization, data usage life cycle, and data hierarchy management in accordance with the aforementioned workflow, combine them with specific business departments and business directions, lay out a reasonable data management structure, and conduct data compliance training for internal personnel (including corporate executives) and external cooperative third parties, so as to gradually form an effective data compliance management system for long-term operation.

3.3. Conduct regular assessments of the effectiveness of data compliance management efforts

The first step is to perform data compliance monitoring. When problems are discovered in the course of work, we take the initiative to reflect them to the management department, which accepts the reports and refers them to the data compliance team for analysis and processing. This ensures that the enterprise's activities of collecting, storing, using, and processing data in its daily business activities are in line with the data compliance requirements stipulated in the relevant laws and regulations of China.

The second step is data compliance auditing. Completed by the internal independent audit department or entrusted to an external third-party auditing organization or professional law firm, through the use of professional and systematic methods, the enterprise's business activities involved in the data compliance management review and evaluation of the scoring, and issue relevant professional opinions on the audit of the problems found one by one to explain the issues, the issues will be categorized by the risk level, and put forward corrective comments and measures for the risk. The audit will explain the problems found in the audit one by one, categorize the problems into risk levels, and propose corrective suggestions and measures for the risks.

The third step is the management review. The top management of the enterprise takes the lead in conducting a comprehensive evaluation of the adaptability, adequacy and effectiveness of the data compliance management system, as well as the implementation of the data compliance policy and objectives, using the results of the analysis in the second step as the criteria and taking into account the actual situation of the enterprise.

References

[1] Chen, R. H. Basic issues of corporate compliance[J]. China law review, 2020(01):178.

[2] Fan Yuan. Experts Interpret 40 Key Points of the Data Security Law [DB/OL]. https://baijiahao.baidu. com/s?id=1702268522687501585&wfr=spider&for=pc.[2022-10-11].

[3] Hanyang District People's Court, Wuhan City, Hubei Province. Hubei Province Wuhan City Hanyang District People's Court (2021) E0105 criminal early 207 criminal judgment [EB/OL].https://wenshu.court.gov.cn/ website/ wenshu/181107ANFZ0BXSK4/index.html?docId=3uFe0YX95zHiQlQh2xoTBtTu/J0gmij0pT6RVIbgXS9HsgWy PdBFnfUKq3u+IEo4GK/X7mouP/yWj1/V8OgBs9Nr/mevkd96dqmup4VlR7xIAhnEmhXFK7M/CrtCCbLz.[2022-10-11]

[4] Jin-Wen Yang, Xin-Hui Wang. Interpretation of the First Data Compliance Non-Prosecution Case and Implications for Corporate Data Compliance [DB/OL]. https://mp.weixin.qq.com/s/hmQiC8M7ZPH3h04OHdOErg.[2022-10-11].

[5] Shanghai Pudong New District People's Court. Shanghai Pudong New District People's Court (2018) Shanghai 0115 Criminal 2974 Criminal Judgment [EB/OL]. https://wenshu.court.gov.cn/website/wenshu/ 181107ANFZ0BXSK4/ index.html?docId= tLWwykCoBI5QkPG2oPH+5XgqBcs7xkcLN8xdYAn+sXc0ucV1 VcmDzvUKq3u+IEo4GK/X7 mouP /yWj1/V8OgBs9Nr/ mevkd96dqmup4VlR7xIAhnEmhXFKx16SToXb4cl. [2022-10-11].

[6] Zhuo Li. Analysis of corporate data compliance issues and countermeasures under GDPR [J]. Northwestern Law, 2020(1):182-196.

[7] Yu Chong. Iterative Alienation of Data Security Crimes and the Path of Criminal Laws and Regulations--The Introduction of Criminal Compliance Programs as a Perspective [J]. Journal of Northwestern University (Philosophy and Social Science Edition), 2020, 50(05):100.