Scientific Research Publishing

Beijing Law Review, 2023, 14, 674-690
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Reflections on Criminal Compliance for Corporate Personal Information Protection

Jun Zhao

Law School, University of International Business and Economics, Beijing, China
Email: zhao8890@126.com

How to cite this paper: Zhao, J. (2023). Reflections on Criminal Compliance for Corporate Personal Information Protection. *Beijing Law Review, 14,* 674-690.
https://doi.org/10.4236/blr.2023.142036

Received: April 14, 2023
Accepted: June 5, 2023
Published: June 8, 2023

Abstract

As legislation related to the protection of personal information continues to improve, the importance of corporate criminal compliance continues to grow. The web crawler uses scenario, data acquisition scenario and data provision to the public scenario are the key areas of criminal compliance for corporate personal information, and it is necessary to identify the corporate criminal legal risks in the three scenarios and implement the related criminal compliance legal obligations. On this basis, we will build a criminal compliance system for corporate personal information protection, identify legal obligations, self-examine existing risks, carry out top-level design and specification development, and build a powerful enforcement tool for corporate personal information protection criminal compliance to ensure daily maintenance and supervision of corporate personal information criminal compliance.

Keywords

Personal Information, Criminal Compliance, Data Protection, Institutional Construction

1. Introduction

In recent years, with the development of the digital economy, criminal cases involving the protection of personal information in violation of the law have shown rapid growth[1]. In order to cope with the severe situation, China's legislature and judiciary have increased the protection of personal information, and the basic legal system of data compliance has been constructed by the Personal Information Protection Law, the Data Security Law and the Network Security Law, which is effectively supplemented by several judicial interpretations. For

[1]Criminal cases involving infringement of personal information of citizens—big data reports, https://m.163.com/dy/article/I11TBCVK05561JEJ.html.

example, the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Infringement of Citizens' Personal Information issued by the Supreme People's Court and the Supreme People's Procuratorate in May 2017; the Notice on Implementing the Personal Information Protection Law and Promoting Public Interest Litigation on Personal Information Protection issued by the Supreme People's Procuratorate in August 2021 and the Provisions on Several Issues Concerning the Application of Law in Hearing Civil Cases Relating to the Use of Face Recognition Technology in Handling Personal Information issued by the Supreme People's Court in July 2021, etc. Criminal compliance of personal information handling is an inevitable requirement of modern corporate governance system in the era of digital economy, emphasizing that companies actively prevent data criminal security risks with their own efforts and eliminate personal information-related crimes with strict management and legal compliance mechanisms. In addition, criminal compliance can also be a criminal excuse, producing the legal effect of non-prosecution or deferred prosecution. For example, in the case of a crime committed by an employee within a company, criminal compliance construction can be a defense to the exoneration or penalty reduction of a unit crime.

2. Examining the Criminal Compliance of Corporate Personal Information Protection from the DIDI Incident

Although the act of "illegal collection" by DIDI is not recognized as "theft" or "illegal acquisition by other methods" and whether the collected screenshot information constitutes a crime cannot be generalized, the possibility that DIDI faces criminal risks cannot be ruled out in theory.

2.1. The Incident of DIDI Being Fined

On June 30, 2021, DIDI was officially listed on the New York Stock Exchange with an offering price of $14. As of July 1, DIDI stock jumped 17%, with a market capitalization of over $70 billion, and was highly sought after by domestic and international capital. But two days later, on July 2, Netflix China released the "Network Security Review Office Announcement on the Launch of Network Security Review on DIDI. The announcement said that the DIDI will implement a network security review, the review period DIDI to stop new user registration. On July 4, 2021, according to reports, the State Internet Information Office found that the DIDI App has serious illegal and irregular use of personal information collection, and therefore notified the application store to take down the DIDI App in accordance with the relevant provisions of the "Network Security Law of the People's Republic of China", and requested DIDI Technology Co., Ltd. to strictly follow the legal requirements, refer to the relevant national standards, and seriously rectify the existing problems, and effectively protect the security of personal information of the majority of users. On July 16, 2021, the State Internet Information Office, together with the Ministry of Public Security,

the Ministry of State Security, the Ministry of Natural Resources, the Ministry of Transport, the General Administration of Taxation, the General Administration of Market Supervision and other departments jointly stationed in DIDI Technology Co., Ltd. to carry out a network security review, and according to the conclusions of the network security review and the problems and clues found, the State Internet Information Office in accordance with the law on the suspected illegal acts of DIDI companies to open a case for investigation[2]. During the period, the State Internet Information Office conducted investigations and inquiries, technical forensics, ordered the drop company to submit relevant evidentiary materials, in-depth verification and analysis of the evidentiary materials in this case, and fully listen to the views of the drop company to protect the legitimate rights of the drop company.

A year later, on July 21 this year, the State Internet Information Office imposed a fine of RMB 8.026 billion on DIDI Global Co. and a fine of RMB 1 million each on Cheng Wei, Chairman and CEO of DIDI Global Co. and Liu Qing, President of DIDI Global Co.[3] in accordance with the Network Security Law, the Data Security Law, the Personal Information Protection Law, the Administrative Punishment Law and other laws and regulations.

2.2. The Importance of Data Compliance Revealed by the Incident

The three laws that the State Internet Information Office relied on in the case of the drop being fined, the Network Security Law, the Data Security Law and the Personal Information Protection Law, together form an important legal basis for data compliance. With the introduction of supporting departmental regulations, administrative regulations and normative documents, data compliance-related enforcement will be more frequent and severe. The Internet department said[4] it will increase law enforcement efforts in the areas of network security, data security, personal information protection, through law enforcement interviews, ordering corrections, warnings, notifications and criticisms, fines, orders to suspend related business, shut down and rectify, close the site, off the shelves, deal with the responsible person and other disposal and punishment measures, according to the law to combat the danger of national network security, data security, infringement of citizens' personal information and other illegal acts, and effectively safeguard national network security, data security and social public interests, powerful protection of the legitimate rights and interests of the general public.

Therefore, once a company fails to do its data compliance work properly, resulting in illegal consequences, it may be ordered to rectify by relevant regulatory authorities or face administrative penalties of the type of warning, fine, sus-

[2]The "DIDITaxi" App Removal Incident: https://baike.baidu.com/item/%E6%BB%B4%E6%BB%B4%E5%87%BA%E8%A1%8CApp%E4%B8%8B%E6%9E%B6%E4%BA%8B%E4%BB%B6/57889803?fr=aladdin.

[3]"DIDI" was fined 8.026 billion yuan, source: CCTV News WeChat public number, "NetLetter China" WeChat public number.

[4]"DIDI" was fined 8.026 billion yuan! Investigation, illegal facts, Punishment basis, Source: Beijing Daily WeChat Public Number.

pension, revocation of business license or related business permit, civil liability, or even face criminal penalties. In addition to the responsibility of the unit, the responsible persons are subject to individual liability, including fines and prohibition from practicing their profession, such as prohibition from serving as directors, supervisors, senior managers and persons in charge of personal information protection of the relevant enterprises for a certain period of time. It is worth noting that the responsible persons do not only include the directors and supervisors in the traditional sense, but also the person in charge of corporate network security and data protection or the person responsible will also bear the corresponding legal responsibility.

2.3. The Illegal Facts of DIDI in the Incident

In the case of DIDI being fined, the State Internet Information Office found a total of 16 illegal facts, which are summarized in 8 aspects: 1) 11,963,900 screenshots from users' cell phone albums were illegally collected; 2) Excessive collection of user clipboard information and application list information 8.323 billion; 3) Excessive collection of passenger face recognition information 107 million, age group information 53.592 million, occupation information 16.3356 million, kinship information 1.3829 million, "home" and "company" taxi address information 153 million; 4) Excessive collection of 167 million pieces of precise location (latitude and longitude) information when passengers evaluate the chauffeur service, when the app is running in the background, and when the phone is connected to the orange view recorder device; 5) Excessive collection of 142,900 pieces of driver education information, and 57,802,600 pieces of driver ID number information stored in plaintext; 6) analyzing 53.976 billion pieces of information about passengers' travel intentions, 1.538 billion pieces of information about their resident cities, and 304 million pieces of information about business/travel in other places without explicitly informing them; 7) frequently asking for unrelated "phone privileges" when passengers use ride-hailing services; 8) failing to accurately and clearly explain user equipment 19 personal information processing purposes, such as information about users' devices.

In addition, DIDI also has data processing activities that seriously affect national security, as well as refusing to fulfill the clear requirements of the regulatory authorities, and other illegal and unlawful issues such as yang-fang and malicious evasion of supervision. The illegal and illegal operation of DIDI brings serious security risks and hidden dangers to the security of national critical information infrastructure and data security, but these issues are not disclosed by the Internet information department according to the law because they involve national security.

2.4. The Development Stage of Legislation Related to the Protection of Personal Information in China Requires Enterprises to Improve Their Compliance Awareness

The penalty decision of the State Internet Information Office on DIDI shows

that the illegal and irregular operation of DIDI brings serious security risk potential to the security of national critical information infrastructure and data security, which is not disclosed according to law because it involves national security. And of the eight aspects of the illegal facts that have been disclosed, one is an illegal act, four are transitional acts, and the other three are unclear acts. This shows that the legislation in the field of personal information protection and data security in China needs to be further clarified and continue to be improved. At present, the legislation on personal information protection and data security is still under development. Under the existing legal system, enterprises should comply with the laws and regulations on the one hand, and strengthen the research and follow-up of the laws and regulations on the other hand, so as to prevent the compliance risks caused by the lack of understanding of the laws and regulations.

It is worth noting that when the regulators imposed penalties, they also imposed penalties on the drops for continuing violations prior to the effective date of the personal insurance law. Therefore, enterprises should strengthen the self-examination of personal information handling history, and when there are many departments and complex links involving the collection and use of personal information, enterprises should promptly self-examine and find and correct situations in which the actual use of business exceeds the scope of privacy rules notification and authorization or other legality-based categories. In particular, APPs and applets should focus on complying with the substantive lawful requirements under the "superficial compliance" initiative of privacy policy notification and consent solicitation to ensure the lawfulness of the actual purpose of data processing and the lawfulness of the collection and use and other processing methods and means.

2.5. Enterprises Should Do a Good Job of Internal Self-Examination and Legal Compliance Obligations to Implement the Risk of Personal Information Protection

From the situation of illegal handling of personal information, the illegal acts of DIDI involve multiple Apps, covering a variety of situations such as excessive collection of personal information, mandatory collection of sensitive personal information, frequent claiming of rights by the App, failure to fulfill the obligation to inform about the handling of personal information, and failure to fulfill the obligation of data security protection. In particular, DIDI performs various types of analysis of user data without explicitly informing users of the purpose and manner of use. Usually, the actual use of data after the enterprise has completed data collection is more secretive, and this is a key task that requires multi-departmental compliance for the enterprise to complete. Therefore, in order to avoid "backroom operations" and ensure transparent and legal rules for data use and processing, companies should promptly detect and correct any violations of privacy rules in the actual use of business.

In order to curb the spread of compliance risks at the source, enterprises

should establish corresponding compliance systems and internal system systems in a timely manner in the midst of collecting and processing data. On the one hand, it connects with the "Network Security Law", "Data Security Law", "Personal Information Protection Law" and other laws and regulations, and on the other hand, it meets the actual requirements of enterprise production and operation. As data security has been raised to the level of national security, China's enforcement of personal information protection and data security will be further enhanced, and the construction of a criminal compliance system for the protection of personal information of enterprises can brook no delay.

2.6. Enterprises Should Timely Response to Regulatory Requirements and Ensure the Effectiveness of Internal Personal Information Protection System

In fact, DIDI has not established a data compliance system within its organization. Although DIDI has set up an information and data security committee, under which there is also a personal information protection committee, data security committee and other bodies involved in the decision-making guidance, supervision and management of the behavior related to the business line of online dating, hitchhiking, etc., but still did not fulfill the obligations of network security, data security, personal information protection in accordance with the relevant laws and regulations and regulatory requirements, and ultimately "bring serious risk potential to national network security, data security", which shows that the internal data compliance system of DIDI has not played its proper role.

3. The Main Scenarios of the Criminal Legal Risk of the Protection of Personal Information of Enterprises

Criminal compliance of enterprises related to personal information mainly involves three scenarios: 1) business related to web crawlers; 2) data acquisition and exchange; 3) external provision of data, especially the case of making metadata of citizens' personal information available to the public, rather than data products. Based on the existence of different business processes and product solutions, the crimes that may be involved in different businesses and products of different companies are all different, and therefore, the criminal compliance tools to be adopted are also different.

3.1. Criminal Legal Risks of Web Crawlers and Corporate Personal Information Protection

Through web crawler technology, companies can automatically crawl the Internet via computers according to their actual needs, thus achieving efficient reading and collection of web information. In terms of the technology itself, the reasonable use of web crawler technology is beneficial to the improvement of work efficiency, but there are legal boundaries for the use of web crawler technology, and the improper use of web crawler technology to obtain non-public data may violate the Anti-Unfair Competition Law, the Network Security Law, the Per-

sonal Information Protection Law and other legal provisions. For example, web crawlers, as an automated program, are more difficult to obtain the consent of the subject whose personal information is collected directly during operation, and therefore need to be particularly careful when the data collected involves personal information (Chang, 2020).

For example, in a case where a technology company crawled personal information without authorization and sold it, the technology company secretly crawled the resume data of job seekers on domestic mainstream recruitment platforms by forming a special crawler technology team without obtaining direct authorization from job seekers and platforms. During the case review process, more than 210 million pieces of personal information with crawler characteristics were found from the data involved in the case. After investigation, the technology company obtained the above data; the data was reorganized and used to develop products with the intention of profit. During the period, the head of the technology company's crawler technology team, Ou, privately sold the company's stolen resume data to the public and personally made an illegal profit of more than RMB 300,000. Finally, the defendant unit, a technology company, was sentenced to a fine of RMB 40 million, the defendant Wang was sentenced to seven years in prison and a fine of RMB 10 million, and the other defendants were sentenced to corresponding penalties[5]. Although web crawler technology has a very important role in promoting the use of data, attention should be paid to the compliance and legality of its use, which is also the proper meaning of personal information protection.

3.2. Data Buying and Enterprise Personal Information Protection Criminal Legal Risk

At the stage of acquiring information, enterprises should, on the one hand, ensure that their data collection practices are compliant, including self-collection compliance and acquisition compliance from third parties, and on the other hand, they should do enough compliance management obligations to avoid the risk of falling into the crime of omission. According to Article 4 of the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information", if a person obtains citizens' personal information through purchase, receipt or exchange in violation of relevant state regulations, or collects citizens' personal information in the course of performing duties or providing services, it falls under Article 253-1, Paragraph 3 of the Criminal Law, which stipulates "illegally obtaining citizens' personal information by other means" (Zhou, Zou, & Yu, 2017). The term "purchase" in this context should be understood in a broad sense, i.e., it should be understood as data transfer and sharing with consideration, i.e., it may occur in data procurement, business cooperation and M&A transactions. Therefore, in

[5][Explaining the law by case] Technology company uses crawler technology to steal 210 million pieces of resume data Haidian District Procuratorate successfully prosecuted to protect citizens' personal information (qq.com), accessed September 13, 2022.]

the criminal law risk of personal information protection, data acquisition involving personal information is one of the important sources of risk.

For example, in a case in Guangdong, defendant Tang himself or instructed his employees to purchase 1,748,903 pieces of personal information from others, and then defendant Tang sold and distributed the personal information to his employees for marketing products and selling. The defendant Liang received personal information from the defendant Tang for telephone marketing of health care drugs and "Jia Lai Pin Pu" brand health care products. The public security authorities seized 74,688 pieces of personal information from the defendant Liang's cell phone. The court held that the defendants Tang and Liang violated the relevant provisions of the state, illegal access to citizens' personal information; the circumstances are particularly serious, their behavior has constituted the crime of infringement of citizens' personal information, should be investigated for criminal responsibility[6]. From the case, it is clear that the defendant Tang violated the relevant state regulations and conducted commercial activities by paying consideration for personal data, which seriously violated the rights and interests of information subjects, i.e., the sale and distribution of shared personal information for commercial purposes is punishable under criminal law.

3.3. Data Provided to the Public and the Criminal Legal Risk of Enterprise Personal Information

After entering the digital economy, data have become an important production resource for Internet companies or data-intensive enterprises, playing an irreplaceable role in technology development, algorithm optimization, user expansion, product or service upgrade and marketing promotion. Since it is difficult for enterprises to grasp all the data in various fields of production and operation, they usually choose to obtain data valuable to them by means of data trading and put the data into use. In the process of data trading, it necessarily involves the provision of data to the public, and enterprises may therefore bear the criminal legal risk of personal information protection. For example, in the Supreme Prosecutor's guiding case Ke infringed on citizens' personal information (Prosecution Case No. 140), Ke was the proprietor of an information technology company in Anhui, which developed the website "FangLiBang". In January 2016, Ke started to operate the website "FangLiBang" and developed a cell phone APP with the same name to sell second-hand houses for rent and sale in Shanghai as the main business. During the operation period, Ke uploaded real owners' housing information to the website members for cash incentives, attracting real estate agents who had such information (dealt with separately) to register as members and provide information to the website, obtaining a large number of owners' housing information containing house numbers and owners' names, telephone numbers and other non-public content for a fee. After acquiring the

[6]See Guangdong Qingyuan Intermediate People's Court (2020) Guangdong 18 Criminal Final Ruling No. 166.

above owners' listing information, Ke arranged for employees posing as real estate agents to contact the owners one by one by phone for verification, and provided the valid information in the form of membership packages to the website members for a fee. In the process of contacting and verifying the information, the above-mentioned employees also failed to truthfully inform the owners of the acquisition and use of the owners' listing information. From January 2016 to the time of the crime, Ke illegally obtained more than 300,000 pieces of property information from owners through the operation of the website "FangliBang" and made profits of more than RMB 1.5 million by selling them in the form of membership packages. On December 31, 2019, the Jinshan District People's Court handed down a verdict, sentencing Ke to three years' imprisonment, four years' probation, and a fine of RMB 1.6 million for infringing on citizens' personal information.

4. Corporate Personal Information Protection Criminal Legal Risk Scenario Compliance

In the early stage of development of the Internet and data industry, although the lag of legislation and law enforcement officers need to understand and learn the process, and the economic value of data is not so prominent, easily resulting in some serious violations do not constitute a crime of "practical experience", but can not use the experience of judgment, industry practice to replace the legal judgment. Industry custom is not a statutory exemption, and the law will not exempt the behavior involved from punishment just because it is customary in the industry. With the increasing awareness and enforcement of the protection of citizens' personal information, enterprises should keep an eye on the trend of judicial decisions in practice, in addition to complying with relevant laws and administrative regulations (Zhu et al., 2022).

4.1. Criminal Compliance for Corporate Personal Information Protection in Web Crawler Scenarios

The criminal compliance of enterprise personal information protection in the web crawler scenario can be analyzed from two aspects: whether to comply with the robots protocol and to set the restriction strategy for crawling content.

If a website is set up with a robots agreement, it should be strictly observed. Although it is still controversial whether it is illegal to crawl in violation of such agreements on websites, caution should be exercised and it is not advisable to break through the anti-crawl technical measures of the target website to avoid committing the crime of illegal acquisition of computer information system data. If a general personal website or commercial website or APP neither sets up anti-crawl technical measures nor makes public anti-crawl statements, the public data of the website is generally crawlable.

In addition to complying with the robots protocol, it is also necessary to set up a restriction strategy for crawling content, and the crawled content should be reviewed promptly after crawling. If the data is found to belong to the user's per-

sonal information, privacy, commercial secrets involving others, or copyrighted works, there is a risk that it may constitute a crime of infringement of citizens' personal information, a crime of copyright infringement, or a crime of commercial secret infringement accordingly, the crawling should be stopped in time and the information already crawled should be deleted in its entirety. If the business models of both parties are the same or similar, and obtaining the other party's information by means of crawlers is likely to cause direct damage to the other party or detract from its expectable interests, the relevant data should not be crawled to avoid the legal risk of unfair competition; if it is the other party's core and bulk main business commercial data, collection by means of crawlers should be avoided as far as possible to avoid harming its substantial commercial interests and violating the relevant provisions of the Anti-Unfair Competition Law, which may lead to legal disputes (Lin, 2020). In addition, special personnel should be set up to manage the crawler software to avoid intrusion into computer information systems in the fields of national affairs, national defense construction, and cutting-edge science and technology.

4.2. Criminal Compliance for the Protection of Personal Information of Enterprises in Data Procurement Scenarios

In the scenario of data acquisition, it is difficult to meet the standard of criminal compliance for the protection of personal information of enterprises, and the problem lies in the fact that the core feature of the act of "illegal acquisition" with "purchase" as the main means is the lack of "consent" of the information subject. The problem is that the core characteristic of "illegal acquisition" by means of "purchase" is the lack of "consent" of the data subject and no other legal basis. Accordingly, when an enterprise obtains data through a third party, it is obligated to review the legality of the third-party supplier's data and keep evidence in order to avoid criminal risks arising from the illegality of the third-party data source. For example, the qualification of suppliers is audited. When purchasing data from third parties, enterprises should ensure that the suppliers are legally qualified and have not been subject to administrative penalties, and should also comprehensively assess the suppliers' data security management capabilities, prior data transaction experience and capabilities, and service quality, etc., and keep audit records. Another example is that the enterprise needs to check the documents proving the legal source of the supplier's data, find out whether the agreement signed between the supplier and the user clearly authorizes, authorizes the scope of use, usage, etc., require the supplier to provide and sign a commitment that the data does not infringe on the personal information and other legitimate rights and interests of others, and agree that the supplier will bear all the losses suffered by the enterprise as a result of the dispute.

4.3. Enterprise Criminal Compliance in the Scenario of Providing Personal Information to the Public

Enterprise data processors should clarify the boundaries and scope of data use in

the process of selling and providing personal information, so that the use of data has a legal basis, otherwise it may constitute a crime of infringement of citizens' personal information. It is worth noting that in cases of illegal sale and provision of personal information, it is not uncommon for unit staff to use the convenience of their positions to carry out illegal and criminal activities. With the strengthening of the protection of personal information, the obligation of enterprises to take corresponding active measures to prevent such acts is bound to gradually increase.

In the scenario of providing personal information to the public, enterprises can avoid criminal risks in the following three aspects: First, compliance training for the business end to provide personal information to the public in different scenarios. When personal information is transmitted to the public, if the specific scenario involves personal bank and deposit information, transaction records, medical consultation records, disease history and other information, the consent of the individual should be obtained and encryption should be adopted. If more than 100,000 pieces of sensitive personal information are provided to the public, a full-time person in charge of personal information protection and a personal information work organization should be established to be in charge of personal information security and ensure that the work is carried out legally and compliantly. Second, when providing data to the outside world, the purpose and scope of processing important data, processing methods, and data security safeguards should be agreed with the data recipient, and the data security responsibilities and obligations of both parties should be clarified by signing a contract. Meanwhile, according to the cooperation agreement signed by both parties, the processing activities of the data recipient shall be always supervised and tracked, and the approval records and logs of the supervision process shall be kept for at least five years. Third, the establishment of a minimum authorized access control policy, the need to set up an internal approval process for important operations of personal information, the separation of roles for security managers, data operators, and auditors, and the over-authorized authority to handle personal information should be approved and recorded by the person responsible for the protection of personal information or the personal information protection work agency.

5. Key Points for Building a Criminal Compliance System for Corporate Personal Information Protection

Through the study of criminal cases on the protection of personal information of enterprises, it is found that in some cases, the employees of enterprises did not violate the information of citizens with the authorization of the unit or beyond the scope of authority, but they used the convenience of their work, at this time, it is controversial whether the enterprise and the person in charge have done enough to manage the obligation and whether they should be responsible. Although some enterprises have successfully defended through sufficient evidence that they have done their management obligations, with the gradual improve-

ment of the data compliance system, the data compliance obligations of enterprises have gradually become clear, and enterprises should be judged by whether their compliance plans are perfect and whether they have been effectively implemented without criteria. The Nestle employee's infringement of citizens' personal information case[7], as the first case of corporate compliance not guilty plea, Nestle's plea successfully provided the basic path for the criminal compliance of data processors, that is, the legal obligation given by laws and regulations is transformed into the internal system of the company. The emergence of the first domestic data compliance non-prosecution case in May this year also provides some guidance for the construction of a criminal compliance system for corporate personal information protection[8]. Enterprises should further improve their management systems and systems in conjunction with the provisions of the Personal Information Protection Law, the Data Security Law and other relevant laws and regulations, actively undertake the obligation of data compliance management, safeguard personal information security, and avoid the criminal legal risk of enterprises falling into the crime of omission due to their failure to fulfill their management obligations.

5.1. The Collection of Personal Information Should Meet the Three Principles of Legality, Clarity of Purpose and at Least Enough

The Personal Information Protection Act provides the basis for the legality of

[7]In 2016, the first trial of the People's Court of Chengguan District, Lanzhou City, found that six employees of Nestle Company, in order to seize market share and promote Nestle milk powder, illegally obtained more than 100,000 pieces of citizens' personal information from medical staff of many hospitals by means of soliciting relationships and paying benefits, constituting the crime of infringing citizens' personal information. After the first trial, each defendant appealed on the grounds that their acts were company acts and the case should be a unit crime. During the first trial of the case, Nestle invoked compliance as a defense. Nestlé argued that it never allowed its employees to collect personal information from consumers in an unlawful manner and never provided funds to employees or medical personnel for this purpose, and that its Nestlé Compliance Charter, Nestlé Instructions (taken from Nestlé's employee training materials), and Graphic Guidelines on the Relationship with the Health Care System clearly state that "medical professionals must not be induced with money or material goods. For these requirements, Nestlé also required all nutrition specialists to receive training and sign a letter of commitment, and had established an effective compliance program. The court concluded that the above compliance documents fully proved that Nestle had fulfilled its obligations of compliance management, had the awareness of avoiding and preventing compliance risks, and had conducted compliance training, and the defendant in this case violated Nestle's compliance management regulations, which should be a personal act. The Court of Second Instance, Lanzhou Intermediate People's Court, also recognized this and ruled that the appeal was rejected and the original verdict was upheld.

[8]From 2019 to 2020, Company Z's Chief Technology Officer Chen and a number of technical staff illegally obtained the data of a takeaway platform for the company's operational needs through technical means such as "external crawl" and "internal crawl" without authorization, causing a direct economic loss of more than 40,000 yuan to the takeaway platform. The technical staff of the company, without authorization, illegally obtained the data of a takeaway platform by "external crawling" and "internal crawling", causing direct economic losses of more than 40,000 yuan to the platform. After the public security authorities submitted an application for early intervention to the procuratorial authorities, the prosecutor decided to carry out data compliance management for the case. On April 28, 2022, the procuratorial authorities held a public hearing on non-prosecution, and on May 10, 2022, the procuratorial authorities conducted a "cloud declaration" of non-prosecution against Company Z, announcing the decision not to prosecute. The case is also known as the first domestic data compliance non-prosecution case.

collecting personal information[9] 1) or based on the consent of the subject of the personal information. The "consent" here has a rich connotation, and various laws and regulations and normative documents have detailed provisions on the scope and form of "consent". According to the Personal Information Protection Act, "separate consent" shall be obtained for "public collection" and "collection of sensitive personal information"[10]; According to the "Personal Information Notification Consent Guidelines (Draft for Comments)", "When collecting personal information, the personal information subject shall be informed of the type, purpose, manner and scope of collection and use of personal information, and the express consent of the personal information subject shall be obtained. According to the "Personal Information Notification Consent Guidelines (Draft for Comments)"[11], "When collecting personal information, the personal information subject shall be informed of the type, purpose, manner and scope of collection and use of personal information, and the express consent of the personal information subject shall be obtained"; 2) or necessary for the conclusion or performance of a contract to which we are a party. The "necessary" here needs to be further clarified, and reference can be made to the "Scope of Personal Information Necessary for Common Types of Mobile Internet Applications"; 3) or necessary for the performance of legal duties or legal obligations; 4) necessary for responding to public health emergencies, or for protecting the life, health and property of natural persons in emergency situations; 5) for the public interest in the implementation of news reporting, public opinion monitoring and other acts, within a reasonable range of personal information; 6) within a reasonable range of personal information that individuals disclose themselves or other personal information that has been lawfully disclosed.

The principle of clarity of purpose. According to the Personal Information Protection Law[12] "the processing of personal information shall have a clear and reasonable purpose, and shall be directly related to the purpose of processing and in a manner that has the least impact on the rights and interests of the individual"; "the processing of personal information shall follow the principles of openness and transparency, disclose the rules for processing personal information, and express the purpose, manner and scope of processing[13]; "if the purpose of processing personal information, the manner of processing and the type of personal information processed are changed, the consent of the individual shall be obtained again[14]". In summary, the purpose of collecting personal information should be clear, disclosed, and consent should be obtained again after the change (if the basis of legality is "individual consent").

The principle of minimum sufficiency. The implementation of the compliance

[9]Article 13 of the Personal Information Protection Act.

[10]Article 26 of the Personal Information Protection Act, Article 29 of the Personal Information Protection Act.

[11]Article 5.1 of the "Guidelines for Informing Consent of Personal Information (Draft for Comments).

[12]Article 6, paragraph 1 of the Personal Information Protection Law.

[13]Article 7 of the Personal Information Protection Act.

[14]Article 14 of the Personal Information Protection Act.

requirements of the principle of necessity and the grasp of the scale are the "hardest hit" areas for enterprises to collect data, especially self-collection. According to paragraph 2 of Article 6 of the Personal Information Protection Law, the collection of personal information shall be limited to the smallest extent to achieve the purpose of processing and shall not collect excessive personal information; the evaluation point 4 of the Self-Assessment Guide for the Collection and Use of Personal Information by Mobile Internet Applications (App) further clarifies the necessity criteria, which are: whether to collect personal information that is not related to business functions; whether users can refuse to Whether the collection of non-essential information or opening non-essential permissions; whether the collection of users' personal information is forced in an unjustified manner; whether the frequency of collecting personal information exceeds the actual needs of business functions.

5.2. Companies Need to Identify Their Legal Obligations and Self-Examine the Existing Risks of Personal Information Protection

With the successive promulgation of legal norms such as the "Network Security Law", "Data Security Law" and "Personal Information Protection Law", the rules of the superior legal framework in the field of data compliance have basically taken shape. From the perspective of risk avoidance, enterprises need to conduct a comprehensive and thorough inventory, combing and identification of compliance issues in their current data processing solutions, and establish a technology application compliance assessment system to avoid technology abuse. On this basis, in order to respond to the requirements set forth in the law, including "data processing risk monitoring and periodic risk assessment of important data processing" as proposed in the Data Security Law, and "impact assessment of personal information protection in specific cases" as required by the Personal Information Protection Law, companies need to form their own internal operation mechanism that integrates their business rules and is effective based on a thorough understanding of the regulations, and incorporate the legal compliance obligations of personal information protection into their internal approval and management processes to help them identify risks and avoid them.

5.3. Enterprise Personal Information Criminal Compliance Needs to Pay Attention to Top-Level Design and Specification Development

In the top-level design of corporate personal information criminal compliance, a unified programmatic system document is essential, and the construction of internal programmatic system documents is not arbitrary, but needs to be built from multiple dimensions, such as the department responsible for management, organizational structure, data security and personal information protection principles, as well as basic technical and operational requirements. In terms of form, the completed internal programmatic system document should be publicly

released in the company's internal staff meeting or other forms in accordance with the law, so that it can become a system known to every internal employee and strictly abide by. In the supporting norms, the network security and data protection obligations of different subjects in the relevant laws are different, and "network operators", "data processors" and "personal information processors" should assume different obligations respectively in the regulations. Based on this, companies need to adapt to the regulations and build their own regulations and norms that can be referred to.

In addition to these, enterprise data classification and grading management regulations, enterprise data source legal compliance review specifications, employee data security and authority management specifications, personal information encryption and de-identification guidelines, data exit security management requirements, network data security emergency response plans and process regulations are all matters that enterprises should consider.

5.4. Enterprise Personal Information Criminal Compliance Needs to Pay Attention to Top-Level Design and Specification Development

To establish a compliance system that meets the legal requirements and intended purpose, it needs to be built at three levels: a better top-level design, sound supporting norms and strong implementation tools. Only by achieving the organic combination of the three can we build a working data compliance system specification system. All three require delicate design by enterprises, especially the enterprise personal information protection criminal compliance enforcement tools, which must be strong and grounded.

Given the breadth and diversity of matters and coverage of personal information protection, building a set of data compliance form recording tools or templates can be very helpful in saving compliance costs and improving compliance efficiency. In addition, in order to improve the efficiency of the compliance work, a set of compliance tools can be designed for the personal information handling record obligation, personal information protection assessment obligation, etc. that can be generalized.

5.5. Enterprise Needs to Ensure the Daily Maintenance and Supervision of Personal Information Criminal Compliance

In terms of internal system maintenance, enterprises should review whether they have the circumstances or conditions stipulated in the relevant laws to set up special departments and persons in charge of network security, data security and personal information protection, and fulfill their legal obligations and assume the corresponding responsibilities in accordance with the requirements of the law. In addition, current legal provisions oblige internal authorities to conduct regular "compliance audits" of data security and personal information protection. It can be said that one of the important elements to maintain the effective operation of the enterprise personal information protection system in the future

is to carry out compliance audits in the data field, mainly by self or entrusted third-party professional organizations, supplemented by mandatory audits by relevant authorities.

In terms of external implementation monitoring, enterprises should establish stable and smooth data compliance consultation channels including regular communication and consultation with relevant authorities and professional third-party organizations so that risks can be delineated in a timely manner even before they are generated. For companies that meet the requirements of the law, such as those that provide important Internet platform services, have a large number of users, and handle complex types of personal information, the companies themselves should actively accept social supervision, not only by establishing an independent body composed of external members to oversee the protection of personal information, but also by regularly publishing social responsibility reports on the protection of personal information as required by the relevant laws (Sun, 2021).

5.6. Enterprises Should Pay Attention to Compliance in Areas Involving National Critical Information Infrastructure and Important Data Security

Enterprises should pay attention to the following three aspects in order to defuse cyber security risks and national security risks: First, it should improve security awareness and awareness of the rule of law, especially it should correctly understand and handle the relationship between maintaining network security and promoting its own development, adhere to the concept of safe development, and build the cornerstone of network security; second, it should continuously enhance the management and assessment of its own operational security, actively compare the relevant provisions of the Network Security Law and the Data Security Law and the Network Security Review Measures listed in Article 10 Security risk factors, make a good pre-judgment and assessment of security risks, management work; Finally, actively declare and cooperate with network security review, where the review conditions or assessment conditions in line with the "Network Security Review Measures" and "Data Exit Security Assessment Measures" should have the obligation to take the initiative to declare and cooperate with the competent authorities to do a good job in security review or assessment.

6. Conclusion

At present, the top-level design of China's personal information protection and data compliance legal system has been basically completed, at the same time, supporting laws and regulations will also be introduced one after another, and enterprises to achieve criminal compliance of personal information protection can avoid the emergence of administrative or judicial adverse consequences. The establishment of a criminal compliance system for corporate personal information protection is not an individual project but a systematic one. In order to establish an effective criminal compliance system for the protection of personal

information, it is necessary for companies to develop an effective program with the help of third-party organizations and professionals, taking into account their existing and future business practices, and to implement the program in a planned manner. The relevance of the work of building a criminal compliance system for the protection of personal information of enterprises has been increasingly strengthened, and the reality of development requires enterprises to carry out high-quality and refined data compliance work. In the wave of the digital era, enterprises need to conduct more in-depth exploration to fully stimulate the innovative value of data and better play the role of data compliance for risk prevention.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Chang, J. F. (2020). *The Legal Boundary of Personal Information Collection Acts in the Criminal Orientation of Data Compliance.* (In Chinese) https://www.kwm.com/cn/zh/insights/latest-thinking/the-criminal-aspect-of-data-compliance-the-legal-boundary-of-personal-information-collection.html

Lin, Z. Q. (2020). *Compliance Points for "Crawlers" Crawling Data.* (In Chinese) https://lawyers.66law.cn/s2114c9e2d7859_i711652.aspx

Sun, F. B. (2021). *Legal Guidance on the Special Obligations of Large Online Platforms: The Example of Article 58 of the Personal Information Protection Law.* (In Chinese) http://www.mzyfz.com/html/1022/2021-11-26/content-1538380.html

Zhou, J. H., Zou, T., & Yu, H. S. (2017). The Understanding and Application of the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens' Personal Information". *People's Justice (Application), No. 19,* 31-37. (In Chinese)

Zhu, X. Y., Wang, W., Gao, Y., & Sun, X. J. (2022). *Can Investors in the Data Space Also Have Criminal Risks?—Enterprise Digital Transformation Risk Compliance No. 5.* (In Chinese) http://www.meritsandtree.com/index/news/detail?id=207