The Perfect Way Of Personal Information Crime Regulation

WenChao Li

Hainan Vocational College of Political Science and Law, Haikou Hainan, 571100, China

Keywords: Big Data; Legal Benefits; Personal Information; Corporate Criminal Compliance

Abstract: In the era of big data, natural persons commit the majority of personal information crimes, but it cannot be ignored that the misuse of personal information by enterprises has exacerbated the complex situation of the data black chain. On the one hand, we should change the single state regulation model to the prevention and control model of co-governance by the state and enterprises, especially Internet enterprises. Make clear provisions on the mitigation and aggravating punishment of unit crimes, and establish the supporting rules of the enterprise criminal compliance system. On the other hand, refine personal information processing rules, give business data ownership, and optimize personal information sentencing standards. The refinement of personal information processing rules aims to clarify the boundaries of personal information protection and helps regulate the chaos in the data industry. Giving enterprise data ownership allows companies to invest more resources to improve data utilization and security, and promotes the development of the data industry and artificial intelligence technology in a benign direction.

1. The Establishment Of Legal Interest In Personal Information Rights

It is recommended that the right to personal information be used as a legal benefit for the protection of citizens' personal information, and the content of the legal benefits includes personal legal interests and social legal interests. The application of personal information rights in criminal justice is broken down into three levels: First, the value orientation of personal information protection is clearly defined in the context of the era of big data. The theory of risk society provides a justification for the advancement of criminal law and the realization of active prevention. Personal information crime, as a product of the development of the risk society era, has the main characteristics of legal crime, profit-making crime, and cyber-crime. Therefore, the legal interests protected by personal information crime It should meet the basic requirements of a risk society. The theory of risk society believes that man-made risks have gradually replaced natural risks as the main disaster threatening human society. The risk of legal interests infringement caused by personal information crime should be highly valued, and then advocate risk management and security value. Taking the right of personal information as the basis of personal information protection, the personal legal interests and social legal interests are included in the protection of criminal law legal interests. The abstract transformation of legal interest categories is based on the uncertainty and extensiveness of the harm of personal information crimes, and the protection of social legal interests by criminal law also embodies the preventive and prerequisite requirements of legal interests in a risk society, so the establishment of personal information rights as personal information protection legal interests meets the practical needs. Second, at the level of criminal legislation, personal information rights are used as the basis to optimize the classification of personal information types, and at the level of criminal law norms, space is reserved for multiple parties and their rights protection in the personal information flow chain. The classification of personal information is actually to classify the subjects and their rights involved in the flow of personal information, and to clarify the boundaries of criminal protection of personal information. On the contrary, the lack of scientific classification of personal information can easily lead to the ambiguity of the scope of protection of this crime and the question of the lack of justification of punishment. The "Interpretation of Several Issues Concerning the Application of Laws in Handling Criminal Cases Infringing Citizens' Personal Information" classifies personal information and sets different levels of incrimination standards according to different categories. This is a positive criminal justice

attempt, but in enterprises the level of default of personal information supervision still needs to be improved. Third, based on the exclusive right of personal information, the system of combining private prosecution and public prosecution may be adopted at the level of criminal prosecution of personal information crimes. From the perspective of comparative law, the United Kingdom and the United States in the Anglo-American legal system mainly rely on public prosecution, while the German and Japanese civil law systems stipulate that they should mainly rely on private prosecution. In detail, for minor personal information crimes, the private prosecution procedure applies, that is, whether the public power organ pursues the actor's responsibility depends on the criminal prosecution of the party. For personal information crimes that reach serious circumstances, it is stipulated as a public prosecution case, and the implementation of laws and public information security are guaranteed by national coercion. The reasons can be attributed to two points: one is based on the exclusive right of personal information in the right to personal information, and the individual has the right to decide in a certain way how to achieve legal interest protection and damage punishment; second, the setting of private prosecution cases can ease tension the use of judicial resources, and can promote the formulation and implementation of multiple legal sanctions. The establishment of the legal interests of personal information rights is not only to shift the focus of personal information protection from privacy to personal rights and property rights, but also to transfer the part of the right to pursue and punish personal information crimes to be exercised by the victim in a manner recognized by the victim restore its damaged interests to the greatest extent.

2. Refine personal information processing rules and give enterprise data ownership

The development of big data technology promotes the convenience of life while also bringing about problems such as information overload and data security. The risk of man-made risks brought by new technical and new technologies has exceeded that of natural risks. It is urgent to control the negative effects of new technologies and new technologies in the form of a system. Through the refinement of information processing rules and the clarification of enterprise data ownership, the data industry is guided to develop in a benign direction. In the processing of personal information, companies should first follow the principles of data minimization and data anonymization, and grasp the relationship between the use and protection of user data. Data minimization requires companies to clearly define the boundaries for collecting and using personal information. Data anonymization requires enterprises to realize the de-identification of data, reduce the risk of data misuse and expand the profitable space of data, which is conducive to the construction of "data property rights system". In practice, companies should conduct third-party assessments of their data anonymity status and the risk of data transaction parties re-identifying personal information to ensure the legal use of corporate data ownership and the controllability of data transaction risks. At the same time, the public authority should focus on monitoring and cracking down on personal identity re-identification, that is, through the use of data license agreements to restrict the use and disclosure of personal information, when violations of the license agreement are found, the law to investigate the re-identification of the perpetrator according to the nature of the behavior responsibility. In addition, in the face of the severe situation of APP misusing personal information, we should not only face the formal shortcomings of the "informed-consent" principle, but also set up exemptions for the "informed-consent" principle. On the one hand, the "informed-consent" principle is amended through anticipation, and flexible space is reserved in legislation to improve the operability of judicial practice. In short, even if the user reads and agrees to the APP's privacy agreement, the APP operator exceeds the authority to collect and use the user's personal information, which is contrary to the reasonable expectations of the user's use of personal information, and can still be regarded as a violation of personal information and bear the corresponding responsibility. On the other hand, promote the diversification of legitimate reasons for data activities. Article 5.4 of China's "Information Security Technology: Personal Information Security Regulations" stipulates that under special circumstances, personal information can be legally collected without obtaining consent, which is in line with the value orientation of the legal interests of personal information rights and reflects the intelligence of enterprises in the era of big

data. The real needs of in-depth product development and application will contribute to the development of China's data industry and worker intelligence technology. However, the special circumstances specified in "Information Security Technology: Personal Information Security Regulations" without the need to obtain consent are more limited. The "informed-consent" principle excessively restricts the use of personal information, so it is necessary to gradually expand the collection, use and justification in the transfer process.

After the above-mentioned processing of the collected personal information, the enterprise can waive certain related obligations, which means that the enterprise that owns the data has the right to possess, use, transfer and profit from the data without having to obtain the user's consent. That is, data ownership. In the era of big data, the extensive collection and in-depth exploration of personal information is conducive to achieving more accurate predictions, which are core competitiveness for enterprises and even countries. The establishment of the legal interests of personal information rights is essentially to comprehensively protect the personal rights, privacy rights and property rights contained in personal information, and the purpose of legislation is to transfer protection and use from a single protection. Therefore, giving the enterprise data ownership, allowing it to use and protect legally processed personal information, and maximizing the use of the economic benefits of personal information within the scope permitted by law, not only is it conducive to companies to improve their own data protection systems and technologies, but also more conducive to the in-depth exploration and circulation of data in accordance with the law promote the healthy development of the data industry.

3. Introduce corporate criminal compliance system to encourage companies to strengthen internal management

The enterprise compliance management system outside the region originates from the theory of risk society, which aims to reduce the risk of enterprise management and positively affect the criminal responsibility, and ultimately contributes to the positive improvement of the business value of the enterprise. Compared with the traditional criminal governance model, the "cooperative governance" model embodied in the corporate criminal compliance system means that the cooperation between internal self-management and external governance puts the responsibility on individuals and overcomes the shortcomings of traditional single external regulatory inefficiency, will be beneficial to realize the positive prevention function of criminal law. From the perspective of legislative practice, the crime of refusing to perform information network security management obligations as stipulated in Article 268 of China's Criminal Law illustrates that the legislators recognize the use of criminal law to promote internal control of enterprises, reflecting criminal compliance part of the concept. From the perspective of state managers, the implementation of corporate criminal compliance systems means an increase in judicial efficiency. The promulgation and implementation of the "Network Security Law" has provided behavior guidance and responsibility allocation for network service providers, but the deterrent effect of administrative punishment responsibility has limited its role in preventing the misuse of personal information. Therefore, it is necessary to effectively promote enterprises to fulfill their internal management obligations through criminal legislation. Specifically, there is an intrinsic relationship between corporate criminal compliance and liability commitment, breach of attention obligations, etc., and incentivizing companies to self-regulate with penalties is a viable path. In short, through careful management of negligence and penalty incentives, endowment of specific personnel as guarantor obligations, etc., careful planning of corporate compliance management is achieved. The enterprise implements compliance management, and proves that it has fulfilled its reasonable attention and evaded its obligations, which can not only be used as a basis for reducing the penalty, but also as a reason for blocking the penalty, which can effectively prevent and control crime while meeting the goal of reducing the strain on judicial resources.

The following three points should be noted in the localization path of the enterprise criminal compliance system: First, whether the enterprise implements compliance management can be used as a basis for mitigating or deterring the penalty, but it should not be a basis for aggravating the

penalty. As mentioned above, regulating the abuse of personal information by enterprises above the designated size is the core of current problem governance. There are many small enterprises in our country, and the level of corporate governance is uneven. Taking the compliance management of enterprises as the legal cause of strengthening penalties is likely to cause injustice. Secondly, from the current legal norms in my country, the corporate compliance system has not been clearly defined as a general corporate obligation. For example, it is only stipulated that the directors of financial institutions and listed companies have statutory internal control obligations, and in practice, the internal control obligations of directors have many problems such as weak operability. In this regard, a team of lawyers needs to be stationed in the company to cooperate with the company's board of directors, senior management, audit department, and various business departments to establish a practical and effective compliance system after fully grasping the specific conditions of the company. When companies face investigations and prosecutions, in addition to providing response services, the team of lawyers can also provide suggestions for improving the company’s violations of laws and regulations, risk distribution, and compliance vulnerabilities. From the perspective of extraterritorial legislation, this will help companies reduce criminal liability Risk and prevention of recidivism. Third, improve the unit's provisions on the reduction or aggravation of quantitative criminal circumstances in the Criminal Code. my country adopts a single punishment system for unit crimes, that is, it only stipulates that units can be fined, and there is no corresponding penalty determination system. As far as the current unit fines are concerned, studies have pointed out that the application of fines across the world varies widely. The problem with China is that the execution rate of fines is low, and more than two-thirds of fines cannot be enforced. In this regard, it may be possible to draw on the experience of the French Criminal Code on legal person sentencing and enforcement systems. For example, the Criminal Code stipulates the conditions and circumstances for the establishment of a recidivism for a legal person, the conditions and effectiveness of the probation application of the legal person, and the elimination of the penalty for the crime of a legal person. Only when the criminal law clearly stipulates the statutory mitigation and aggravating punishment of unit crimes, measures including corporate compliance can have the opportunity to be included in the scope of sentencing. In short, compared with foreign experience, enterprise compliance management system is in its infancy in my country. Criminal law legislation regards enterprise compliance as an incentive mechanism to encourage enterprises to follow norms and operate legally, which is a feasible countermeasure against the misuse of personal information by enterprises.

Conclusion

The proposed perfect path of personal information crime regulation is based on scientific and rationality, and forms a personal information governance model with Chinese characteristics in the process of continuous optimization, in order to escort the development of my country's big data industry.

References

[1] Xiang Dingyi, Comparison and Enlightenment: Research on the Normative Mode of Commercial Utilization of Personal Information in the European Union and the United States [J], Journal of Chongqing University of Posts and Telecommunications (Social Science Edition) 2019 (4): 48-50.

[2] Huang Xiaoliang, on the abandonment of the concept of "unit crime" in my country-with extra-territorial comparison as the starting point [J], Politics and Law, 2015 (3): 38.

[3] Chen Ruihua, Three Dimensions of Enterprise Compliance System-Analysis from the Perspective of Comparative Law [J], Comparative Law Research, 2019 (3): 69-70.

[4] Li Bencan, Domestic Law Expression of Criminal Compliance Concept-Taking "ZTE Incident" as an entry point [J], Legal Science (Journal of Northwest University of Political Science and Law),

2018 (6): 99.

[5] [Germany] Ulrich Qibai, Criminal Law in Global Risk Society and Information Society [M], Zhou Zunyou, Jiang Suyi, China Legal Publishing House, 2012: 252.

[6] Chen Xiaodong. The path to strengthen the procuratorial supervision of the execution of property punishment [J]. People's Prosecution 2017 (19): 76.

[7] Wen Libin, Innovation and Optimization of Criminal Protection of Personal Information Rights [J], Journal of Chongqing University of Technology (Social Science), 2018 (10): 93-100.

[8] Jin Yao, the legal basis and norm remodeling of personal information to de-identify [J]. Law Review 2017 (3): 120-130.

[9] Wen Libin, the experience of local legislation on personal information protection and the way to achieve it [J], South China Sea Law, 2019 (3): 82-89.

[10] Lin Huanmin, Dilemma and Outlet of the Informed Consent Principle in the Protection of Personal Information [J], Journal of Beijing University of Aeronautics and Astronautics (Social Science Edition), 2018 (3): 17-19.

[11] Wen Libin, the establishment of the crime of invading the citizen information system in the era of big data [J], Theoretical Monthly 2017 (10): 101.

[12] Xiong Moulin, Recognition of my country’s Fine Penalty Jurisdiction——A Tracing Study Based on Cross-Country Comparison (1945-2011) [J], Tsinghua Law, 2013 (5): 110-111.