Data Security Law From The Perspective of Criminal Law

Yuxue Wu[1*]

[1] Law School, Bohai University, Jinzhou, Liaoning, China

Email Address

774674892@qq.com (Yuxue Wu)
*Correspondence: 774674892@qq.com

Received: 7 Ocotber 2022**; Accepted:** 22 Ocotber 2022**; Published:** 25 November 2022

Abstract:

Since the Data Safety Law was included in the legislative plan, it was passed on June 21, 2021 after three deliberations. This indicates that data has been recognized as a new type of independent protection. The introduction of the Data Safety Law also means the further improvement of the national legal system, and it is also a challenge to the corresponding part of the criminal law in China. How to make the criminal law and the new Data Safety Law applicable to each other has become the issue that must be put forward and the situation we are facing. This paper will analyze the Data Safety Law from the perspective of criminal law and put forward relevant suggestions based on the relationship between the two laws.

Keywords:

Data Security, the Era of Big Data, Criminal Law

1. Introduction

With the advent of big data, the development of society and science and technology has long arrived, the Data Safety Law of the country is to make the solution of data security problems more clear and specific, so that the solution of related problems can have laws to follow, in line with the dual justice of entities and procedures.

2. The Background of the Data Safety Law

The rapid development of technologies such as sensors, digital storage, computers, communications, and the Internet has driven an inevitable “big data revolution”. [1] The Data Security Act has emerged just over many years later. “Data” as used in this Law means any record of information in an electronic or non-electronic manner. [2]The subjects carrying out data activities should take necessary protection and safeguard measures from the whole process from data collection to data use until data disclosure, so as to ensure that data is effectively protected and legally used, so that they have the ability to guarantee continuous security status, and help the international competition of China’s digital economy.[3] In recent years, the digital transformation and upgrading of China’s industry has been accelerated, which puts forward new requirements for data security protection. The current legislation on data security issues is blank in China, the legal system is not perfect, and the data security is seriously threatened. For a long time, data is often regarded as a part of virtual property, and is included in property cases for regulation, and the independent value of data security has not been fully reflected in the legislation. In 2017, data security issues were included in the Network Security Law for the first time, laying a foundation for the realization of data security in the field of network security. However, the "Network Security Law" is not a special legislation for data security issues, it only from the network data security, personal data security and national data security three aspects of the data security issues in principle provisions, is not systematic and comprehensive. In addition, in order to make up for the lack of supervision, local governments have issued a series of local documents on data security issues, such as the Shenzhen Special Economic Zone Data Regulations (Draft) and the Tianjin Municipal Data Security Management Measures (Interim). The above local documents regulate the local data market to some extent and play a positive role in maintaining the local data security. However, due to the virtual nature of the data itself and the expanding coverage of the digital economy, most of the data processing activities will go beyond the limitations of the traditional geographic boundaries. The uneven levels of protection and regulation may put the data market into chaos, thus hindering the normal development of the digital economy. In the era of vigorous development of digital economy, a unified data security legal system should be established to improve the effectiveness of data security protection, and lay a solid legal foundation for promoting the development of digital economy.

In the information age, "data risk" has become a new social risk factor. [4] These have posed new challenges to the management of network security, data security and other countries, and data security, as an independent legal benefit, has gradually been recognized by legislation. [5] In this case, the introduction of the Data Safety Law can be said to be very necessary and an inevitable development process for China and even the whole world. Although the digital age has arrived, information development is also very fast, but on the whole is still in its infancy, the system is not sound, understanding does not reach the designated position, unbalanced development, technology is not self-control, incomplete consciousness, insufficient problems such as talent, on the whole, data development and data security overall environment still has problems.

3. The Significance of the Data Safety Law

3.1. Fill in the gap in legislation

At present, "the connotation and extension of national security are richer than at any time in history, the time and space are broader than at any time in history, and the internal and external factors are more complex than at any time in history." Although China has existed in the "Network Security Law" before, but the law for the provisions of the data is not comprehensive, specific, in the large use of data and rapid development of today, the "Network Security Law" has obviously not been enough to build a safe and orderly data application environment. The Data Safety Law was born in the context of the legal network, and it is a law that must be observed for data development in cyberspace. As we all know, there are two ways of rule of law and governance in the real social governance. The so-called governance is to govern related behaviors through moral constraints and ethical constraints. Since the real society and the network society have been integrated, the governance in the real society also needs to be implemented and implemented in cyberspace. The Data

Safety Law makes clear the constraints of governance, which reminds all practitioners to fully consider the issues of social ethics and ethics under the premise of strengthening the legal system in the process of data development and processing. The passage of the Data Safety Law fills the gap of the basic law in the field of data security protection in China, and improves the legal system of data security protection in China. The implementation of the Data Safety Law will enhance the legislative level of data security protection, form a unified data security protection system across the country, and effectively safeguard China's data security. For enterprises, the Data Safety Law will further standardize the data factor market and provide a good market environment for enterprises to conduct cooperation and competition. In addition, this law brings enterprises' data processing activities into the legal scope, and clarifies the basic principles that enterprises should abide by and the basic obligations that they should undertake, which can effectively prevent enterprise behaviors from breaking through the red line of data security protection. For enterprises that suffer from illegal infringement, the Data Safety Law will provide institutional protection for them to safeguard their legitimate rights and interests. For individual users, the Data Safety Law will regulate the processing activities of citizens' personal information and protect their personal privacy from illegal infringement. The implementation of the data safety law can not only regulate the behavior of data collection, avoid indiscriminate, mining citizens'personal privacy information, from the source to prevent the outflow of citizens' personal information, and can also regulate the use of data, set up an effective protection mechanism to protect the citizens 'personal information, to prevent citizens' personal information is illegal dissemination and use. In the future, the Data Security Law will also connect with the Network Security Law, the Civil Code and other laws through its relevant supporting measures, which will help to form a perfect data security protection system and protect the security of citizens' personal data and information.

Therefore, the data of safety law is inevitable, this law not only fill the legislation on data security management, and improve the security of the network space governance legal system, make the governance of data can have laws, at the same time to the data security crime deterrent, so as to reduce the crime rate of data security.

3.2. Expand the scope of data protection

Previously, the protection of data in the Cyber Security Law remained only in electronic data, not non-electronic data. The limitation of this protection was not obvious at the time of legislation, but now this limitation is obviously increasingly large, limiting the positive role of data in economic development. The new Data Safety Law not only provides for electronic data, but also protects and provides for non-electronic data. Improving the limitations of the Cyber Security Law here, this move is undoubtedly another progress in our national legislation.

3.3. Promoting the development of the market economy

For the reasonable and effective use of data will greatly improve the level of economic development in our country, but due to the field of legislation makes the lack of clear legal constraints, data utilization in data utilization, a lot of criminals use legal loopholes or due to the law punishment is lighter and not afraid of crime, for illegal interests desperate, challenge the law, and now the data law will effectively solve the problem, also can make the data in the clear legal environment to more efficient operation, and standardize the market order, promote the market steady development. The Data Safety Law is expected to provide a legal basis for subsequent relevant legislation and provide clear compliance guidelines for general market entities by clarifying basic systems such as data classification and hierarchical management, data security risk assessment, monitoring and early warning, emergency response, and data security review. Therefore, the introduction of the new law is constructive to the market and China’s legal system.

4. Related Cases

4.1. The country’s first “crawler” technology intrusion into the computer system crime case

A “crawler” is a program or script that automatically captures information in a network according to certain rules. Legal “crawler” can improve the efficiency of data collection, greatly promote the development of the Internet economy, but the illegal “crawler” has a very great harm, it will illegal access to website data information, lead to normal operation, make the crawl site out of the control of the network operators, seriously disrupt the order of the Internet economy.

In this case, the plaintiff is: Beijing ByteDance network technology co., LTD., the defendant is: Shanghai sheng product network technology co., LTD., because the defendant cracked the plaintiff's data security protection measures, through false identity into the plaintiff's Intranet, through improper means got the plaintiff insider only know advanced data information, cause the plaintiff company large amount of losses. Finally, the defendant company constituted the crime of illegally obtaining the computer information system data, and punished the person in charge directly responsible and the person directly responsible. In This case, because the plaintiff company has a certain social visibility, and has won the attention of more people and the social public media, so that the society further saw the importance of data security protection.

4.2. An overseas consulting and investigation company secretly collected and stole shipping data case

In 2021, China’s national security agency staff through investigation and analysis and tracking test found that a foreign overseas consulting company for a long time with some personnel keep private and close contact, after an emergency investigation, the overseas company through high pay and other rich reporting lure some criminals in our country for its theft, its shipping confidential information revealed to the overseas company, mainly for: the basic shipping data, specific ship loading information. After the foreign company illegally obtained the data, it was all available to foreign spy groups. The above personnel sold China's confidential information to overseas organizations for their own personal gain, ignoring China's national security, and the nature of the behavior is extremely bad.

The Data Safety Law defines the legal responsibility of illegal data processing in the form of law, which can provide relief channels for large-scale data leakage, illegal data trading, illegal data crawler, unfair data competition and other cases that occur frequently in recent years, and effectively protect the legitimate rights and interests of data subjects. At the same time, the severe punishment of the Data Security Law will ring the alarm for the majority of market operators, forcing the organizations to carry out data processing activities to pay more attention to data work, and create a safe environment for the development and utilization of data. Data security includes personal data security, enterprise data security, and national data security. The above two cases discuss the importance of combining data security and criminal law from the two aspects of enterprise data security and national data security, respectively. Only when the management of data security can be combined with the management of criminal law, can the role of data security management be truly played to the maximum extent.

5. The “Data safety Law” Issued and the Criminal Law Adjustment Suggestions

The introduction of the Data Safety Law means that our country has clear legal norms for systematic management in data security and data management. Under the unified legal system, a new laws and regulations will inevitably affect its other related laws, criminal law as a supplementary law and security law nature of basically all aspects of the social law, the data safety law will undoubtedly affect the provisions of data security, therefore, the criminal law on data security changes with The Times is inevitable. Some suggestions to amend the data security provisions in the criminal law are be below.

5.1. Expand the object of data security protection in the criminal law

The identification of a certain crime is based on the most important protection of legal benefits as the core, explaining its constitutive elements, and measuring the interests under the legal framework of criminal punishment. [6] Some scholars believe that the “data” in the Data Safety Law does not involve financial data, economic data, statistical data and other quantitative data, and its regulatory objects should be limited to the “electronic data” formed or stored in the electronic media, rather than “non-electronic data”. [7] Some scholars also believe that “the Data Safety Law mainly deals with the relationship between enterprises and other enterprises and individuals, and mainly protects the legitimate business interests of enterprises for data”. [8] In my opinion, these are not desirable. The introduction of the Data Safety Law is not only to protect the interests of a part of the social entities, namely the commercial entities, but also not only to protect the electronic data. Through articles 285 and 286 of the Criminal Law, we can see that the protection of data security in China's criminal law is limited to “the data stored, processed or transmitted in the computer information system”, and the data security protected in the Data Security Law refers to “any record of information in electronic or other ways”. Compared with the scope of data protection in the Data Security Law, the scope of the criminal law is significantly narrow. Criminal law only to protect the electronic data in the computer, for the computer electronic data and electronic data is no provision, according to the criminal law “law not crime” principle, for the computer electronic data and electronic data should not constitute a crime in the criminal law, this obviously does not conform to the reality, cause the provisions of the criminal law and the data security law, the same legal system is different, this is obviously unreasonable, it is about data security it is necessary to improve the criminal law to protect the scope of the object.

5.2. Expand the protected means and behavior in the criminal law data security

Criminal law related to data security charges only for computer information system storage, processing or transmission of three stages of illegal access behavior in the regulation, and the data safety law in the whole link from collection to public data protection, punishment for the data implementation of tampering, destruction, leakage, illegal access, illegal use of behavior. Obviously, the latter provisions are more reasonable, and the crackdown on illegal acts is more thorough, more in line with the development of the current society, and the provisions of the criminal law appear to be somewhat out of touch with the rapid development of the society. Of course, the law has the basic characteristic of lag, which is something we cannot change, but we should timely improve after we find the problems, so that the law is more fair and just. Therefore, we should expand the data security crime means and behavior stipulated in the criminal law to promote the justice and fairness of the judiciary.

5.3. Establish a hierarchical and classified data protection system in the criminal law

Data law benefits increasingly show social publicity. According to Article 21 of the Data Safety Law, the state is ready to conduct better protection and management for the protection of data security through the method of data classification and hierarchical protection. [9] However, the criminal Law has not been amended accordingly to meet the relevant provisions of the Data Safety Law. Criminal law of related data crime conviction and sentencing does not distinguish the data level, type and the number of data, so, in violation of the basic principles of the criminal crime, related crime governance and useless will even hinder the data security law play its maximum value, therefore, suggest that criminal law according to the relevant provisions of the data safety law establish data classification component protection system, maximize the function of data security protection, combat the illegal behavior of related data crime. First of all, the first step can be divided by data types, for example, into transportation, finance, housing, shopping, etc., and then further subdivided according to the object, scope and degree of influence, to establish a new system of hierarchical classification and classification protection step by step. Then, all kinds of data are classified separately, according to the importance of the data and the possible impact of data loss or leakage: particularly important data, important data, and general data. Especially important data means data that data directly concerns national security and public interest; important data is data that may affect national security and public interest; general data affects the rights and interests of individual citizens, legal persons or unincorporated organizations. At the above level, we prioritize the protection of particularly important data, followed by important data, and finally, general data. And according to this level of classification to take protective measures and punishment measures for criminals. It can also reduce the cost of running the law. [10] It is also the trend of The Times to establish hierarchical and classified protection policies. Reasonable use of hierarchical and classified protection system can be made more scientifically managed, which is a good way for us to innovate. On the contrary, if not specific data classification protection, make the relevant data protection criminal law always abstract, based on the nature of the data itself, is greatly increase the difficulty of the judicial organs, and protect the purpose of the data security and the direction is inconsistent, therefore, we should actively promote data classification protection system change, make the data protection system provisions more specific and transparent, this is the meaning of the law to play the protection function, and we want to achieve the goals and tasks.

5.4. Establish the data security protection obligations of data processors from the criminal law

Data security risk assessment, reporting, information sharing, monitoring and early warning system, which is the core of the data security system. Data security is a kind of preventive protection against potential security risks, so it is not a passive defense, but an active intervention, so the core of data security protection is to establish a whole-process security control mechanism. The first is the assessment of security risks, especially those for important data processing. Processors of important data shall carry out regular risk assessment of their data processing activities in accordance with relevant regulations, and submit the risk assessment reports to the relevant competent authorities. The risk assessment report shall include the type and quantity of important data processed, Data processing activities being conducted, Data security risks faced with them and their countermeasures; Second, the risk reporting system, Data risk discovery in data processing activities, Report it to the relevant departments immediately according to the safety management system, Relevant departments should analyze and analyze the risks reported, Make the corresponding disposal measures; Third, security risk information sharing, Data security is systematic, Data security risks on a certain node, It may pose global risks to the whole system, Therefore, the data security risk information sharing mechanism should be established among different departments; Finally, the monitoring and early warning, Important data processors and regulators, All need to establish monitoring and early warning mechanisms, Strengthen the acquisition, analysis, analysis and early warning of data security risk information.

The Data Safety Law has clearly stipulated the obligations of professionals to manage data safety, such as the establishment of a unified management and use system, regular training, sampling inspection, etc. If the corresponding people violate their obligations, they should be punished accordingly. Criminal law also stipulates that refused to fulfill the obligation of information network security management crime, to protect the security of network data information, but in the data safety law has been introduced today, the corresponding charges in the criminal law is some thin, suggest that criminal law further refine the crime standard, if the manager will data leakage, because of the complexity of the data itself makes criminals cannot effectively use the illegal data, so data managers should be convicted? In other words, is the subjective requirement of the data security protection of the data processor's obligation intentional or negligent? Does it include negligence? Is the data security protection of the data processor's obligation the behavior criminal or the result crime? If it is stipulated as a result offender, but the data handler does violate his due safety management obligations, but is not guilty because of the lack of capacity or other objective reasons failed to complete the crime. If it is criminal, is it too strict with a data processor? It should be pointed out that whether it is the technical protection obligation or the improvement of the management system, the failure of the obligation will not directly lead to criminal crimes. In most cases, administrative punishment is given, and only refusing to rectify and causing serious consequences will constitute a crime. From the above can be summarized to implement the obligation of data security protection process is: study through the laws and regulations, according to establish their own safety management system, form suitable for their own safety training ability and reserve and form the training mechanism, to carry out the personnel thought, consciousness, ability, etc of training, supporting and perfect some technical measures and other safeguard measures. The above process starts round and round again, forming a cycle. Over time, the data security protection ability of the data processing units will be greatly improved. According to the legislative thought of the newly issued Data Safety Law, it is suggested that the above situation should also be included in the crime of the criminal law to highlight the unity of the law.

6. Conclusions

The data security law on the criminal law can not only promote legislation, also can be clear behavior should be punished by law, criminal law deterrent and guiding role, deter criminal ideas timely stop their crime ideas and crime, and guide all the citizens 'thoughts and behavior, tell the public what behavior is right, what behavior is absolutely not allowed, and promote the progress of citizens' thought and violated data security behavior.

The introduction of the Data Safety Law is a major change in China's legal structure. China's laws will be more and more perfect, and this law can also further protect China's national interests, social interests and citizens' personal interests. The judicial application of the Data Security Law still needs time to polish, but this move undoubtedly makes China's legislative structure a big step forward.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this article.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

References

[1] Mayer-Sch ö nberger V, Cukier K. Big data: A revolution that will transform how we live, work, and think. *Houghton Mifflin Harcourt,* 2013, 18.

[2] Article 76, Item 4, of the Cyber Security Act, provides that the.

[3] Ge, X. Security Research Institute of China Academy of Information and Communications Technology: "<Data Safety Law> Highlights Interpretation, and implementation Outlook".

[4] Jing, L.J. The Expansion and Limits of the Protection Scope of Collective Legal Interests in Information Network Crime. *Politics and Law,* 2019, 1.

[5] Liu, Y.F.; Liu, S.Y.; Li, C. Research on the Protection of Criminal Law of Network Data under the Vision of Compound Law Benefit. *Application of Law,* 2019, 21.

[6] Cui, Z.W. "Legal Benefit Identification and" Plot "Evaluation: Another Way of Interest measurement acting on the crime formation judgment". *China Journal of Criminal Law,* 2020, 5.

[7] Permit. Data security Law: Positioning, Position and institutional structure. *Economic and Trade Law Review,* 2019, 3, 52-66.

[8] Mei, X.Y. Private law limitations and public rank of data protection between sharing and control the sequence construction was performed. *Chinese and Foreign Law,* 2019, 4, 845-870.

[9] Huang, D.L.; Hu, W.H. China's Data Security Legislation Situation, Difficulties and Countermeasures - The Data Safety Law (Draft). *Journal of Beihang University (Social Science Edition),* 2020, 6.

[10] Sun, G.H.; Yang, S.B. The division of public and private law and the internal structure of the law. *Legal system and Social Development,* 2004, 4, 100-109.