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

DOI: 10.23977/law.2024.030205
ISSN 2616-2296 Vol. 3 Num. 2

Legal Interests of Computer and Data Security in the Context of Digital Economy Advocation of Dualism

Shaobo Cui, Zhangwei Yao

Zhuhai City People's Procuratorate, Zhuhai, Guangdong, 519000, China

Keywords: Damaging computer; information system; data crime; data classification; legal benefit correction

Abstract: The current protection mode of computer security and data security adopted in China's criminal law not only causes the crime of "data interference type" damaging computer information system to lack clear extension and contraction in practice, but also is difficult to cope with the new trend of information technology development under the background of Internet 3.0, and can not effectively realize the multi-directional protection of data. Based on this, the data security should be raised in criminal legislation from the appendage of the computer information system to an independent legal interest, the implementation of dual protection of computer security and data security, to the safe operation of the computer information system as a protection law to restore the criminal function of the crime of damaging the computer information system, and through the data classification, pre-law reference and other ways to build the data crime system.

1. The raising of problems

At present, the unified protection system for computer security and data security adopted by China in the criminal law system, that is, the criminal legislation model of integrated protection of data as the appendage of computer information system. The illegal acquisition, tampering and destruction of data in reality are regulated by the crime of illegal intrusion into computer information system, the crime of illegal acquisition of computer information system and the crime of damaging computer information system. Among them, the "interference with data" regulated by the crime of damaging computer information lacks clear criminal law extension. In addition, in judicial practice, the requirement for the result of "causing the computer information system to fail to operate normally" in this crime is relatively broad. As a result, once the behavior of data infringement occurs in reality, the judicial organ will give priority to applying the data protection provisions of the crime of computer information system destruction for regulation. Thus, the current situation of confusing computer crime and data crime into one regulation in our criminal law is formed.

Take "Zhuang interference driving training system case" as an example: Zhuang developed the "E-driving pass" platform through the actual control company, which is used to collect the data of driving school students participating in the training and upload it to the driving training public service network, and the traffic management department confirms whether the driving school students have obtained the driving qualification through the relevant data[1]. After that, Zhuang

Mou and others developed to crack the "E driving pass" software, fictitious driving school students training "driving platform AIDS", and to the driving school students to solicit business, from which a total of more than 230,000 yuan. For Zhuang's above behavior, the court held that: Zhuang et al. developed and used "driving platform auxiliary tools" to upload false data to the public network of driving training services, which is prohibited by law as "increasing the storage, processing or transmission of data in the computer information network system without permission". The consequences of the behavior have infringed on the authenticity, integrity and availability of the data stored, processed and transmitted in the computer information system of others, it should be punished as the crime of damaging the computer information system.

The appearance of the above-mentioned precedents is actually due to the fact that in practice, our criminal law integrates "data" only as an appendage of computer information system, and lacks criminal law norms to regulate data crimes separately. In such cases, we can only expand the crime of destroying computer information system to deal with the trend of data illegal acts. The mode of protecting data security with the help of computer crime can no longer meet the actual needs of data crime governance, and it is also causing the crime of damaging computer information system and other crimes to show an irrational trend of "pocketing" abuse due to the breakthrough of basic text.

2. The limitation of the unified protection of computer security and data security in criminal law

2.1 The pocketing of the judicial application of the crime of damaging computer information system

For example, in the case of "Zhuang interfering with driving training system" mentioned above, although the "driving training public service network" affected by Zhuang's behavior belongs to software, it is included in the broad sense of "computer information system". However, it is worth debating that although the "driving training public service network" in this case was affected by Zhuang's behavior of transmitting false data, the basic data processing function of the website "receive-story-operation" as a piece of software for students' driving learning is still operating normally. In fact, it is the website operator who is affected. The purpose of its operation can not be fully realized because of the defects of the program. In other words, if Zhuang's behavior is to be characterized as the crime of destroying computer information system, it is necessary to expand the interpretation of "computer information system" from concrete to abstract, from a real data processing tool to a "human-computer interaction activity" coupled with the designer's intention and computer function. The rationality of this expanded interpretation is undoubtedly facing the doctrinal question of confusing the interests of this crime's protection law[2].

Admittedly, illegal acquisition, tampering and abuse of data will not only infringe on the personal rights and interests of data owners or legitimate users, but also damage the social governance order of gradual informationization. It is an inevitable trend of The Times to include data security into the vision of protecting social life in criminal law, while judicial organs are constrained by the normative gaps of data crimes in criminal law. Caught in the dilemma of the absence of the protection function of criminal law if indulging such data wrongful acts, and the lack of criminal liability basis if convicted regulation, the judicial organs obviously choose to expand the interpretation of computer crime related charges and flexibly interpret the behavior of "interfering with data" as "damaging computer information system". However, it is obvious that using the expanded interpretation of computer crime related charges to regulate data lawfulness does not apply to the current situation of the development of the data industry, but causes the "pocketing" of computer information system-related charges.

First, as the basic requirement of the original crime of crime and punishment, the clarity of the

crime is directly related to the effective play of the function of the code of conduct and the function of judgment and responsibility of the criminal law[3]. The practice of expanding the interpretation of the crime of destroying computer information system to accommodate the situation of "interfering with data" does not clarify which data belong to the data worthy of criminal law protection in the broad sense, nor does it clarify which data behaviors belong to the "interfering" in violation of criminal norms, and the abstraction of normative judgment is bound to pocket the judicial application, the reason is: "Interference", as an abstract concept lacking formal and stereotyped form, is the integration of all the causes that cause the results to be inconsistent with the presupposition. In other words, as long as there is an objective result of data obstruction, the cause behavior can be identified as "interference" behavior, which undoubtedly causes the data protection in criminal law to fall into the "objective imputation" misunderstanding. As a result, some scholars have questioned the phenomenon of frequent judicial use of "interference" as a backstop of this crime[4].

Second, in the information age, the interaction between any computer information system is essentially the interaction of data, and the friction of data control also occurs all the time between operators and software users, between different operators and even between different users. For example, the behavior of web crawlers will inevitably interfere with the efficiency of data operation of others while repeatedly copying and climbing data of others. The bundled installation behavior imposed by software developers on users will also interfere with users' computer resources. Among the above data behaviors, some belong to the civil tort in violation of the Civil Code, and some belong to the administrative illegal acts in violation of the administrative regulations such as the Anti-Unfair Competition Law and the E-commerce Law. However, Article 286 of China's Criminal Law adopts the one-size-fits-all "violation of state regulations" for the reference of the preposition law, which not only lacks the distinction of the level and adjustment type with the help of blank crimes, but also blurs the boundary between general and criminal violations, resulting in excessive intervention in the field of data circulation by the criminal law, which is not conducive to the healthy development of the information industry.

2.2 The limitation of legal interest protection for the crime structure with data carrier as the object of protection

The legal protection value of "data" is obviously beyond doubt at present. With the development of information technology and digital industry, production and life in the current society can be expressed and transformed in digital form. Data is not only the electronic carrier of citizens' personal information, intellectual property rights and other personal and property rights, but also the most basic production factor in the digital economy. It has independent economic value.

However, just because the concept of "data" contains multiple types of interest value, the concepts projected on the law also have strong legal interest compound and variety. From the perspective of data subordinate sources, it can be divided into personal data, commercial data and public data. From the type of information contained in the data, it can be divided into personality data, computer operation data, property interest data, identity authentication data and so on. Taking foreign experience as a reference, in order to protect different data legal interests, Germany has formulated the "Hessen Data Protection Law" as early as the 1970s to provide special protection for personal data. Later, it has successively adopted the "Federal Data Protection Law" and "General Data Protection Regulation" to link up with the criminal law, separating data into "personal data" and "general data" for separate protection. Another example is the United States, which has a highly developed information industry, classifies and protects data in different fields such as government information, citizen privacy, finance and medical care, and has formed a data governance system

with civil, administrative and criminal hierarchical regulations.

Considering the external legislative reference and the actual situation of the rapid development of China's information industry, it is necessary for the criminal law to form a standard system for multi-directional protection of emerging data legal interests from the perspective of effectively regulating multiple types of crimes against data. As mentioned above, the existing criminal legislation in terms of data protection is still stuck in the inherent legislative model of the early development era of the computer industry, placing "data" security in the crime of destroying the computer information system and other computer security crimes to carry out ancillary protection, as pointed out by some viewpoints: This mode narrowly limits the vision of criminal law in regulating data crimes to the carrier of data, that is, the computer information system, and only emphasizes the technical attribute of data not being infringed on its carrier, while "ignoring the legal attribute that the internal information content of the data should be protected". Obviously, it is out of step with the development of China's information industry which has gradually entered the "Internet 3.0"[5].

Based on this, the current crime structure of China's criminal law taking data carrier as the object of protection not only has the problem of aggravating the pocketing trend of crimes such as damaging computer information system, but also causes the limitation of data protection due to the single norm:

First, it weakens the value of the independent protection of data legal interests. The criminal legislation under the data carrier protection mode only looks at the relationship between computer information system and data from the technical point of view, processing and processing, and does not look at the relationship between procedure and result, tool and purpose from the Angle of legal value: As an important auxiliary tool in production and life, the technical security of computer information system, which is not subject to illegal intrusion, control and destruction, indirectly affects many rights and interests of individuals, businesses and even social public behind it; However, after removing the problem of technical security, the information content of data itself still involves the specific legal interests of citizens, such as personality, property and intellectual achievements. It can be seen that data legal interests and computer security legal interests not only cross the path of legal protection, but also have the social value of independent protection by law.

Second, as a result, some data that is not carried by traditional computers cannot be protected by regulations. With the information industry gradually entering the Internet 3.0 era, due to the in-depth development and wide application of blockchain, cloud computing and other technologies, the interaction of electronic data is gradually decentralized. Under this background, data is no longer limited to the traditional computer information system as the carrier. If the existing crime of illegal control and destruction of computer information system is used to regulate the behavior of endangering data. It is bound to continue to expand the technical explanation of "computer information system", and even further expand from tangible physical equipment to a more macro information network, which obviously will continue to break through the semantic category that the public can understand, contrary to the principle of legal punishment.

Third, can not effectively realize the classification and classification of data protection. Due to the complex and diverse nature and types of data, including personality data, property data, confidential data and other data whose value has been confirmed by other laws, it is obviously impossible to realize the light and orderly classification and protection of data corresponding to different types of legal interests by simply protecting the data as an appendage of the computer information system. And it will cause some of the worthless computer redundant data and cache data to be included in the scope of protection, resulting in unnecessary expansion of criminal law.

3. The perfection of criminal law based on the dual protection mode of computer security and data security

At present, China's information industry is accelerating the formation of a new "Internet 3.0" ecology, and the extensive network topology is constantly expanding the scope of data security risks. In the case that the existing criminal law of computer information system-related charges can not meet the needs of data security, it is necessary to respond to technological innovation and the development of The Times from the legislative level. From the unified protection model that protects data as an appendage of computer information system, to the dual protection model that attaches equal importance to both data security and computer security. Specifically, in order to recognize the independent legal interest value of data security, we should clarify the relationship between "computer information system" and "data", restore the normative function of the crime of damaging computer information system, and re-formulate the related crime system about data security.

3.1 The scope of application of the crime of destroying computer information system is corrected

3.1.1 Rectification of legal interests: the rationality of the theory of safe operation of computer information system

Around the protection law interests of the crime of destroying computer information system, there are the following controversial viewpoints in the academic circles:

First, the theory of data security. The theory that the essential function of the computer information system is to process the data, and what this crime protects is the integrity, authenticity and availability of the computer data as well as the legitimate rights and interests of the owner of the data[6]. Although this theory pays attention to the legal interest value of data security, the understanding of the development of the Internet and data industry still remains in the lagging understanding of defining data as an appendage of computer information system.

The second is the theory of computer information system management order. This theory holds that since this crime is stipulated in the special chapter of the crime of disrupting social management order, its corresponding legal interest should be the state's management order of computer information system[7]. The main defect of this view is that the instrumental nature of computer information system raises it to a vague collective legal interest, which not only blurs the distinction between criminal law and computer administrative law, but also causes the legitimate rights and interests of computer information system owners and legal users to be inadequately protected.

Based on the thinking that the criminal law should realize the dual protection of computer security and data security, this paper holds that the safe operation of computer information system should be taken as the legal interest protected by the crime of damaging computer information system, for the following reasons:

First, the reason why the computer information system can become the protection object concerned by the law from the simple property attribute is that the computer can effectively combine the cognitive ability of human beings and the computing function of the machine to realize efficient automatic data processing. Its high degree of auxiliary function has made all fields of modern society inseparable from the support of the computer. Therefore, it is necessary to take the legal and policy means of "hitting early and hitting young, criminal law first" to ensure the stability and order of human production and life by ensuring the safety of computer operation as a production and life tool. Therefore, taking the normal operation of computer information system as

the legal interest of this crime conforms to its functional orientation and legislative purpose in the criminal law norm.

Secondly, taking the safe operation of the computer information system as the legal interest of the law can clarify the objective result requirements of the crime and reasonably limit the scope of application of the crime. The crime of destroying computer information system stipulated in Article 286 of the Criminal Law of our country is a typical result crime, only when the related behavior causes a certain harmful result can constitute this crime. Although the crime of "causing the system to fail to run normally" has a certain fuzziness, but from the Angle of legal interests of the safe operation of the computer information system, the computer information system is composed of hardware and software, according to a certain logic algorithm automatically processing data equipment. Review of the serious damage to its security operation is concerned about whether the basic tool performance of the computer can objectively operate normally in accordance with the established mechanism, in judicial practice is nothing more than two points: one is whether the hardware peripherals are physically damaged, the other is whether the basic operating system, application programs and other software in the established running program is damaged. Compared with the data security and computer management order, it is obvious that the objective results of the crime can be concretized and clear.

3.1.2 The limitation of the result elements: the objective operation obstacle of "program logic"

The reason why the crime of "data interference" type destroying computer information system has a large number of extensibility cases in practice is that the abstract use of "interference" lacks the clear extension scope of criminal law terms. It also lies in the fact that the judicial practice confuses the subjective and objective distinction between "whether the system can operate normally according to the established mechanism" and "whether the intention of the system designer can be realized normally" when considering the outcome elements of this crime. And when we strictly take the safe operation of computer information system as the protection law of this crime to guide the constitutive elements and the application of the test, the above problems will be reasonably limited.

At present, the mainstream view in theory believes that the process of computer operation is "the processing process of data acquisition, conversion and output by the computer information system with the help of hardware equipment in accordance with the preset program logic and application objectives"[8]. There is no doubt that hardware facilities are the physical basis of any computer information system to achieve the basic operation, through physical means to damage the computer information system hardware equipment resulting in the safe operation of the computer information system hindered, obviously in line with the outcome of the crime. However, the crimes against computer security in judicial practice are mainly concentrated in the field of computer software. According to the above definition, in practice, there are two points to judge whether the software of computer information system is "damaged" in the sense of criminal law: "program logic" and "application target".

As mentioned above, under the framework of the dual protection of computer security and data security in criminal law, computer security protected by criminal law refers to the performance security of computer as a tool, that is, to ensure that computer information system can normally realize its data processing function according to the preset program logic. After the system designer completes the design of the computer system, whether the design purpose can realize the non-inevitable expected benefits, itself does not belong to the scope of criminal law protection, and the judicial system does not have the obligation to make up for the design fault of the system designer afterwards; What's more, the constitutive elements of criminal law should be specific, clear and predictable, that is, when protecting the normal operation of computer functions, criminal law can only protect the objective procedural logic that the system designer has expressed through the

form of code, but cannot protect the subjective intention that the system designer has not manifested in the program design and retains in his heart. Otherwise, the constitution of this crime depends on what the inner thoughts of the system designer are, and it violates the conclusion of the principle of crime and punishment.

3.2 The construction of criminal law system to regulate data crime

3.2.1 Criminal law protection structure based on data classification

When China enacted the Data Security Law in 2021, it was clearly proposed that the state should establish a perfect data classification and classification system, requiring different levels of protection for ordinary data, important data and core data. This systematic idea of data governance is exactly what criminal law needs to inherit when participating in data governance, because data legal interest is not a single, isolated type of legal interest. It is "a collection of legal interests directly related to the data in various ways of expression or resource carriers", which means that the different types of infringed data not only affect the difference in the "quality" of the damaged interests, but also affect the difference in the "quantity" when the criminal law evaluates the social harm, so it is necessary to implement the criminal law protection of classification and classification of data[9].

First, for the data involving national security and major public interests, the criminal law configuration of "behavior offense + result aggravation" is implemented. According to the Data Protection Law, "data related to national security, the lifeblood of the national economy, important people's livelihood, and major public interests" should be more strictly regulated and protected. However, the criminal law, as the last line of legal defense for important legal interests, lacks corresponding charges. Although the first paragraph of Article 285 of the Criminal Law makes it a crime to intrude into computer information systems in the fields of "state affairs, national defense construction, and cutting-edge science and technology", this only provision can only protect specific computer information systems. There are not only difficulties in identifying the nature of computers, but also problems such as single responsibility for behavior. Moreover, it neglects the protection of relevant important data that does not use the above-mentioned computer as the carrier. Therefore, it is necessary to carry out criminal protection around the important and core data of the state itself, and criminalize the act of "illegally acquiring and holding" important and core data of the state in the form of behavioral crime on the basis of Article 285 of the Criminal Law.

Second, improve the criminal law protection of data use links involving personal information. Although the crime of infringing citizens' personal information is stipulated in Article 253 of the existing Criminal Law, the behavioral elements regulated by this crime are limited to the illegal acquisition, sale and provision of data transfer, and there is no criminal regulation on the illegal use of personal information. At present, the mainstream view is that the right to personal information is a personal legal interest linked to citizens' personal life, property security and personal privacy. In the era of big data, the most serious infringement on the relevant factual interests behind citizens' personal information often occurs in the link of illegal use. From the stage of infringement of legal interests, in the data circulation link, the acquisition, sale, provision and other acts belong to the dangerous crime stage of "causing illegal use of citizens' personal information". Based on this, Article 253 of the Criminal Law lays too much emphasis on the regulation of data circulation while ignoring the regulation of illegal use of data, which obviously puts the cart before the horse. Therefore, it is necessary to further improve the crime of infringing on personal information in the data use link[10].

Third, the property data should be covered in a way that protects the overall data security order. The so-called property data refers to data that is recorded and expressed electronically or in other

ways and can directly or indirectly generate economic and social value, including processed big data products, digital currency and traffic data. Because whether data can become the object of property rights in civil law is still to be considered at present, and the value attribute of data exceeds the traditional property ownership, and it is difficult to achieve the duration of property protection and other problems, so in the case of the Internet 3.0 related industrial structure has not been completed and mature. Administrative regulations such as the Civil Code, the Anti-Unfair Competition Law and the Data Security Law should be taken as the first step, shifting the focus of criminal law from the ownership of data to the legal control of data, further clarifying the standards and conditions under which property data illegally acquired, used and damaged by others' legal control should be subject to criminal law regulation, and forming the backstop guarantee norm for data security order in criminal law[11].

3.2.2 Taking the advance law in the field of data management as reference, improve the related charges of data crimes in the criminal law

In the field of data protection, China has successively formed the "Data Security Law" and "Personal Information Protection Law" and other laws, while the "Network Data security Management Regulations" and the national standard "Information Security Technology Important Data Identification Guide" and other documents are also gradually improved, providing an effective pre-law reference basis for the identification of data crimes. Further, in order to reduce the overlap or conflict between different laws and regulations, and to clarify the boundary between civil, administrative and criminal wrongfulness of data acts, it is necessary for criminal law to take the pre-law of data management and protection as a reference, and form a double-layer protection path of "civil -- administrative -- criminal law" in the entity and procedure:

The supervisory department should improve the connection identification of data types, levels and identification standards between the advance law and the advance law. As pointed out above, data crime involves multiple levels of legal interests such as individuals, society and the state. Although there is an irreconcilable contradiction between the highly extensive social relations adjusted by the criminal law and the limited legislative capacity of the criminal law itself, it is necessary to use the pre-law to sort out different data. The supervisory department should further improve the essence, connotation value and conceptual scope of legal interests referred to by different data types. For example, although the crime of infringing on citizens' personal information in the existing criminal law and the Personal Information Protection Law adopt a consistent connection between the connotation and extension scope of personal information, as some scholars have pointed out. The criminal law, the Civil Code and the Personal Information Protection Law are still incongruous and even disjointed in terms of the grading standards of personal information and the "factual interests" carried by personal information. Therefore, the criminal law should further take the professional provisions of civil law and administrative law in the field of data as a reference, take the new data rights and interests that have been proven in the civil field as the basis and maximum scope, and select the new legal interests that meet the normative purposes of the criminal law from the perspective of the proportionality principle of criminal law and complementarity[12].

4. Conclusions

Criminal law participation in data governance should follow the principle of proportionality, while protecting the rights and interests of data, it should also preserve the necessary freedom space for the orderly circulation and development of data. The data crime is a legal crime, and its double violation structure determines that when some data behavior is confirmed as legal by the advance

law, it should also be criminally excluded. That is to say, when the criminal law constructs the related charges of data crime with reference to the advance law, it should simultaneously transform the exclusion rules of the advance law to the exclusion causes of crime. For example, once personal information is self-disclosed by a natural person, that is, after the scope of privacy has crossed over to the scope of publicity, the criminal law can neither adopt absolute equal protection for the disclosed personal information of others to avoid the imbalance of interest distribution between the data subject and the data processor, nor can it completely put such data into "open data" to give up protection. Otherwise, it will cause serious violation of the data subject's right to self-determination and abuse of their personal information, which requires the pre-disclosure law to provide effective normative guidance[13-15].

References

[1] Xu Chuncheng, Lin Tenglong. Legal Interest Debate on the Crime of destroying Computer Information System from the doctrinal Perspective [J]. Science and Law (Chinese and English), 2023(04):21-31.

[2] Li Huaisheng. The Change of legal Interest of Data Security and the regulation of Criminal Law [J]. Jiangxi Social Sciences, 2023, 43(07):33-44.

[3] Xia Wei. On the Legislative reconstruction of Data Crime [J]. Legal and Social Development, 2023,29(04):173-190.

[4] Wang Huimin. Dilemma and Solution of Data Crime Governance in China [J]. Northern Law School, 2023, 17(01): 122-132.

[5] Liu Shuangyang. The typification of data legal interests and the construction of Criminal Law protection System [J]. China Journal of Criminal Law, 2022(06):37-52.

[6] Liu Xian-quan. Reconstruction of Criminal law Regulation of Computer System in the era of "Internet 3.0" [J]. Journal of East China University of Political Science and Law, 2022, 25(05):67-78.

[7] Yan Erpeng. Judicial Determination of the crime of disrupting Computer Information System [J]. China Journal of Criminal Law, 2022(03):122-137.

[8] Yu Jian. Criminal Law Regulation and Value Recognition of property Data [J]. Law, 2022(04):78-87.

[9] Wang Huawei. Doctrinal Reflection and Reconstruction of Crime of destroying Computer Information System [J]. Journal of Southeast University (Philosophy and Social Sciences Edition), 2021, 23(06):93-104+147.

[10] Chen Xingliang. The types of cyber crimes and their judicial recognition[J]. Rule of Law Research, 2021(03):3-16.

[11] Su Sanyi. From data carrier to data information: the regression of legal interest standard of data security [J]. Journal of Southwest University of Political Science and Law, 2019, 22(06):97-108.

[12] Zhou Libo. Judicial Practice analysis of crime of destroying computer information System and adjustment of Criminal law norms: An Empirical Study based on 100 judicial cases [J]. Rule of Law Research, 2018(04):67-76.

[13] Zhang Mingkai. Legal interest protection and proportionality principle [J]. Social Sciences in China, 2017(07): 88-108+205-206.

[14] Sun Daoci. Review and prospect of Big Data legal benefit Protection in criminal law [J]. Journal of Central South University (Social Science Edition), 2017, 23(01):58-64.

[15] Wang Shizhou. Modern penalty objective theory and China's Choice [J]. Legal Studies, 2003(03):107-131.