Journal of Contemporary Educational Research, 2022, Volume 6, Issue 4
http://ojs.bbwpublisher.com/index.php/JCER
ISSN Online: 2208-8474
ISSN Print: 2208-8466

Reconstructing the Data Crime Governance Model from the Perspective of Criminal Compliance

Qianshi Wang*

Hebei Normal University, Shijiazhuang 050024, Hebei Province, China

***Corresponding author:** Qianshi Wang, wangqianshi@163.com

Abstract: With the advent of the risk society and the era of big data, criminal law must respond to data crime in a more proactive manner. The traditional way of conviction and sentencing adopted by the current criminal law for data crime can no longer meet the requirements of the times. Compliance should be introduced into criminal law to improve the governance system of data crime. There are three ways to incorporate compliance into criminal law: (1) as the exemption cause of enterprise crime; (2) as the general circumstances of sentencing in the General Provisions of Criminal Law of the People's Republic of China; (3) as the special circumstances of sentencing in the Specific Provisions of Criminal Law of the People's Republic of China. The latter two approaches are more suited to China's national conditions.

Keywords: Criminal compliance; Data crime; Governance model; Risk society; Era of big data

Online publication: April 29, 2022

1. Introduction

Criminal compliance is not only an enterprise management model, but also a criminal incentive mechanism. In particular, an enterprise practices compliance management in accordance with the provisions of criminal law to avoid violating the criminal law and committing a crime. Once an enterprise is truly suspected of committing a crime, the judicial organ can be indulgent since the enterprise has practiced compliance management, thus encouraging the enterprise to continue practicing compliance management. In recent years, domestic research on criminal compliance can be divided into two contexts: the first includes research in the field of procedural law, mainly focusing on the non-prosecution system [1-5]; the second includes research in the field of criminal law, mainly focusing on the discussion of unit crime [6-8].

2. Technological development poses new challenges to the data crime governance model

2.1. Data crime presents a new modality as a result of technological development

With the development of internet technology, the world has entered the era of big data. The advent of the big data era has brought human society into an ultramodern digital society. In the so-called digital society, data technology has changed people's way of life and thinking. Almost all activities can now be digitalized, having significant economic and strategic value [9]. This fact has not only brought great changes to people's production and life, but also made data crime undertake a more complex form. Specifically, the direction of data crime in the era of big data is no longer just the addition, modification, deletion, and interference of data stored, processed, and transmitted in computer information systems, but has evolved into a multi-behavioral pattern major criminal system centered on big data objects, which vertically infringes on the double-layer legal interests of technology and reality; its negative repercussions affect all levels –

individuals, society, nation, politics, military, and the fields of property, personal, and democratic rights [10]. From the perspective of the object of crime, the object of data crime has evolved from a small amount of determined data in the past to massive and fuzzy big data. Often, after data processing has been completed, the data processor has no idea what data it has processed, but the unauthorized processing has caused great harm and may have even constituted a crime. From the perspective of legal interests infringed by crime, what data crime infringes is not only personal rights, property rights, and other personal legal interests, but also social and public interests, as well as national sovereignty, security, and development interests. Such changes condition that the governance of data crime should not be complacent, but rather to follow the trend and fulfil the demands of the times.

2.2. A single data crime governance model in the criminal law

As one of the means of social governance, criminal law primarily regulates people's behavior by stipulating crime and penalty, so as to achieve the dual purpose of punishment and crime prevention. China's current criminal law holds on to the traditional model in the governance of data crime, in that it stipulates which behaviors, using data as the object of infringement, constitute a crime, and it is matched with corresponding penalties to punish data crime behaviors, serving as both general prevention and special prevention. In *Criminal Law of the People's Republic of China*, data crime refers to the illegal acquisition, deletion, modification, and addition of data, including the crime of illegally acquiring computer information system data in Paragraph 2 of Article 285, as well as the provision of deleting, modifying, and adding data in Paragraph 2 of the crime of destroying computer information system in Article 286 of *Criminal Law of the People's Republic of China* [11]. In addition, data crime in a broad sense, which means the specific object infringed may be data as a carrier, mainly includes the crimes of trespassing on computer information systems, infringing personal information, infringing trade secrets, and obtaining state secrets illegally. For big data companies, the most commonly committed crimes in judicial practice are crimes of illegally invading computer information systems, infringing on citizens' personal information, and refusing to perform the obligation of information network security management [12]. Regardless of the discussion whether the criminal constitution of these crimes can meet the requirements of data crime governance or not in the era of big data, the current governance means of criminal law for these crimes are mainly after the fact that they can only be convicted and punished if relevant criminal acts occur. However, it is insufficient to prevent the occurrence of these crimes and to mitigate the harm caused by them.

2.3. Criminal legislation should meet the requirements of the times for data crime governance

From the standpoint of the criminal rule of law, we are confronted with the tasks of modernization and post-modern dimensions; we must prevent arbitrariness outside the law and restrict the power of national penalty, as well as manage the insecurity in the risk society and strengthen safety protection [13]. Some scholars view that what criminal cases are to legal theories (at least some of the legal doctrines) is equivalent to what enemy aircrafts are to missiles that are intended to intercept the enemy aircraft in batches. The missiles must possess the flight complexity equivalent to that of the flight behavior of the enemy aircraft, in order to be able to intercept the aircraft [14]. Similarly, the complexity of criminal cases determines the complexity of criminal law theories. Otherwise, complex practical cases cannot be solved by too simple theories and legislative designs. Data crimes in the era of big data are more complex than traditional crimes. On the one hand, the complexity of data application and the diversity of data analysis and mining escalate the issue of data ownership management and in resisting security attacks; on the other hand, more and more cross-organizational data circulation further aggravates the security risk of data theft, misuse, and abuse [15]. It is clear that relying on traditional legislative models cannot solve the prevention and control problems of data crimes completely. In order to adapt to the complexity of data crimes, the field of criminal law in China

urgently needs to look for new methods to deal with the changes over time. At this stage, implementing criminal compliance is a good option.

3. The introduction of criminal compliance as an inevitable requirement for data crime governance

3.1. A call for criminal law to play a more active role with the advent of the risk society

With the advent of the risk society, the protection model of criminal law has gradually transformed from post-governance to pre-prevention. From the legislative concept, the functional characteristics of contemporary criminal law legislation are extremely obvious; legislators respond more quickly and have a stronger desire to control society through criminal law [16]. In terms of legislative content and frequency, criminal law expresses a proactive attitude in revising and improving the content and frequency. This shows the function of criminal law in protecting society and actively preventing crime [17]. Traditional criminal law theories place a greater emphasis on the importance of special prevention and negative general prevention [18]. However, the driving force of punishment and deterrence alone is often insufficient to manage people's conduct. Traditional criminal law theories hold that the initiation of criminal law should be complementary and guaranteed, which implies that only when civil law, administrative law, and other norms are unable to address a problem can criminal law be used to solve it. However, with the advent of a risky society, in order to prevent more potential social risks, criminal legislation has steadily transformed to a positive one. Some new offences in recent criminal law revisions, for example, are responses to the positive perspective of criminal law. Now that the criminal law has begun to play a more active role in crime prevention, there should be better ways to urge people to intentionally fulfill their legal obligations and avoid being accused of committing crimes, except for adding charges and punishing criminal preparations. Criminal compliance is one such strategy that takes the regulation of corporate behaviors and the prevention of corporate crimes as its starting point and goal, as well as fits the risk society's standards for positive criminal law.

3.2. The concept of criminal compliance is highly consistent with the governance requirements of data crime

If criminal compliance is an inevitable trend of criminal law development in the risk society, defining the natural relationship between criminal compliance and data crime governance is insufficient. After all, in the risk society, the risk is not just data risk, and criminal compliance can prevent more than just data crime. Why is the introduction of criminal compliance an inevitable requirement of data crime governance?

(1) Criminal compliance is an idea, or a management mode used to prevent corporate crime. In the era of big data, enterprises, as processors of massive data and data security obligors, are more likely to commit crimes due to their illegal processing of data or failure to fulfill their data security obligations. Therefore, criminal compliance and data crime meet at the point of corporate crime.

(2) Criminal compliance is also a means of criminal governance. Its criminal governance strategy is primarily to provide "preferential treatment" to enterprises that have formulated effective compliance plans to reduce criminal responsibility, so as to encourage enterprises to carry out compliance management and avoid violations of laws and regulations. No matter whether the concept of "risk society" is recognized or not, there is no doubt that compared with traditional risks, the risks in modern society reflect the artificiality, agnosticism, and severity of the consequences [19]. Given that data crime has the characteristics of incalculable loss in the era of big data (the use of leaked data by criminals may engender serious personal and property crimes or even bring harm to national security), post-punishment is not enough to prevent and control the harm caused by data crime. The best way of governance is for enterprises to standardize data processing activities from the source and prevent data

crimes as much as possible. Here, the role of criminal compliance perfectly meets the needs of preventing data crimes.

3.3. Reduce the harm of data crime with the introduction of criminal compliance

Although it is expected that the introduction of criminal compliance will effectively regulate the data processing behaviors of enterprises and urge them to actively fulfill their data security obligations, it is apparent that this strategy cannot completely eliminate data crime. Even so, the introduction of criminal compliance can help to mitigate the harm caused by some inevitable data crimes. First, the introduction of criminal compliance can reduce the harm of data crime to victims. In the era of big data, each and every person's personal information resides on the network in the form of data, and this information may be used illegally at any time. In this sense, everyone is a potential victim of data crime. If the criminal law stipulates that enterprises can gain leniency by implementing certain remedial measures for previous corporate crimes, companies will then endeavor to make up for losses and avoid further violations of the rights of victims. Second, the introduction of criminal compliance can reduce the harm of data crime to enterprises. Since data crime is typically defined by the premise that the behavior violates pre-existing laws (such as the Personal Information Protection Law, Data Security Law, and so on), enterprises that commit data crime face not only criminal liability, but also severe administrative penalties, including loss of business qualifications if serious, which is unquestionably a fatal blow to enterprises. Third, the introduction of criminal compliance separates corporate responsibilities from employee responsibilities; that is, once a data crime occurs, if the company can prove that it has developed an effective compliance plan and put it into practice, and the data crime is caused by the failure of employees to execute compliance, the enterprise can escape being a victim of data crime. This is beneficial to the preservation of the enterprise's strength.

4. China's criminal law introduces the models of compliance in the governance of data crime

European and American countries use compliance as the incentive mechanism of criminal law, which can be divided into five modes: (1) non-prosecution based on compliance; (2) compliance as the reason for innocence defense; (3) sentencing based on compliance; (4) exchanging compliance for a settlement agreement, resulting in the withdrawal of prosecution; (5) exchanging the disclosure of illegal acts for lenient criminal punishment. Among them, the first and fourth are both in exchange for compliance with the prosecution's non-prosecution in the litigation procedure, which are issues of concern to the procedural law [20]. The other three are the reduction or exemption of the criminal entity's responsibility in exchange for compliance, which are issues that the criminal law should pay attention to. When combined with China's criminal law's crime and punishment systems, three legislative models are available for selection when introducing compliance.

4.1. Taking compliance as the exemption cause of enterprise crime

Criminal compliance legislation should be based on the premise of building an independent unit crime system. When the consequences of endangering society caused by acts committed by natural persons in the name of the unit can be attributed to the internal governance structure and operating mode of the unit, the unit shall be investigated for criminal responsibility. On the contrary, only natural persons shall be investigated for criminal responsibility [21]. China's criminal law follows the principle of the unity of subjectivity and objectivity. When affirming a crime, if the subject does not have a subjective crime (intentional crime or negligence), it cannot constitute a crime. The establishment of this principle means that China's criminal law does not recognize no-fault liability but recognizes constructive liability in individual charges (such as the crime of an unidentified source of a huge amount of property). On the premise that the criminal law can recognize constructive responsibility, there is possibility to appoint the

compliance as the defense of innocence. First of all, it is necessary to determine the constructive responsibility of the enterprise; that is, when the relevant responsible persons have committed a criminal act for the interests of the enterprise, the enterprise is presumed to be culpable. It stipulates that the enterprise can take compliance as defense; that is, if the enterprise can prove that it has formulated an effective compliance plan and implemented it, the enterprise is not required to bear criminal responsibility of the unit crime for the criminal acts of the employees. This constructive crime can also be introduced into the enterprise's data processing activities; as long as the enterprise has violations of laws and regulations in data processing, it is presumed that the enterprise has committed a crime. However, if the enterprise can prove that it has formulated an effective compliance plan, and the relevant employee has failed to execute the plan, resulting in data crime, then the enterprise will not be held criminally responsible for the data crime as the criminal subject. Although this model can reduce the legal responsibilities of enterprises and employees, there are also some hidden dangers. For example, in order to avoid becoming the subject of crime, enterprises would make minor sacrifices to safeguard major interests by holding some employees criminally liable. Even if the enterprise does not do so, the behaviors of employees reflect the enterprise in the eyes of the public. Even if their behaviors are not influenced by the enterprise, the enterprise has regulatory responsibility. If an enterprise implements a compliance plan, it cannot be held criminally liable, which is unavoidably unacceptable to the public.

4.2. Taking compliance as the sentencing circumstance in the General Provisions of Criminal Law of the People's Republic of China

Compared to taking compliance as the exemption cause of corporate crime, it is easier for the public to accept taking compliance as the sentencing circumstances of corporate crime in China. In the 1980s, the Federal Sentencing Commission of the United States stipulated that if an enterprise has established an effective compliance plan, the punishment can be reduced when a crime occurs [22]. This practice is known as "sentencing incentive." There are many "sentencing incentives" in the General Provisions. For example, criminals who surrender themselves can be given a lighter or mitigated punishment, and those who commit a lighter crime can also be exempted from punishment. The "lighter, mitigated or exempted punishment" refers to a lenient punishment on the premise of determining the guilt of the criminal. Even if the punishment is exempted and the penalty is not imposed, the "guilt" of the criminal is not denied. The existence of such sentencing circumstances has played a role in encouraging criminals to start with a clean slate and reduce the harm of crime. It has been widely accepted by the public. When compliance is introduced into criminal law, it can be regarded as a lenient sentencing circumstance specifically applicable to enterprise crime in the General Provisions. The circumstances of compliance leniency can be divided into two categories: pre-event and post-event. For enterprises that have formulated and implemented effective compliance plans before the crime, the leniency may be greater; for enterprises that have actively formulated and implemented effective compliance plans after the crime, they will also be given a certain leniency. Of course, whether or not the enterprise's compliance plan submitted as a sentencing circumstance can be accepted by the court may only be determined after a thorough review and appraisal by a third-party evaluation organization.

4.3. Taking compliance as the sentencing circumstance in the Specific Provisions of Criminal Law of the People's Republic of China

There are also many "sentencing incentives" in the Specific Provisions of Criminal Law of the People's Republic of China. For example, criminals who commit the crime of corruption and bribery, if they confess their crimes truthfully, sincerely repent, and actively return stolen goods before filing a public prosecution, they may be given a lighter or mitigated punishment or even exempted from penalties altogether. This kind

of circumstance is different from the scope of sentencing circumstances in the General Provisions, and the legislative purpose also differs. The sentencing circumstances in the sub-rules are designed for specific crimes. For example, in the case of corruption and bribery crimes, which involve obtaining large sums of property and having a negative impact, relying on heavy penalties alone is not the best way to minimize criminal loss. Taking the crime of corruption as an example, if the huge amount of public property embezzled by criminals cannot be recovered, the losses of the state and the people cannot be compensated only by heavy penalties (even, the death penalty). Therefore, when dealing with such serious corruption crimes, there are higher expectations for the criminal law, hoping that it will not only punish criminals, but also erase the sufferings brought by these crimes. The "sentencing incentive" clause was born at the right moment. Designing targeted compliance sentencing plans for specific crimes in the sub-rules for data crimes would better highlight the role of compliance in data crime governance.

Disclosure statement

The author declares no conflict of interest.

References

[1] Chen R, 2020, Compliance Incentive Model of Criminal Action. China Legal Science, 2020(6): 225-244.

[2] Li Y, 2021, Legislative Suggestions on Conditional Non Prosecution of Enterprises. Criminal Science, 2021(2): 127-143.

[3] Li H, 2021, Non Prosecution of Enterprise Compliance: Misunderstanding and Correction. China Law Review, 2021(3): 177-188.

[4] Chen R, 2021, Eight Controversial Issues in the Reform of Enterprise Compliance Non Prosecution. China Law Review, 2021(4): 1-29.

[5] Li Y, 2021, Applicable Cases of the Corporate Compliance Non-Prosecution System. Legal Forum, 2021(6): 21-30.

[6] Wan F, 2019, Development and Enlightenment of Criminalization of Enterprise Compliance. Criminal Science, 2019(2): 47-67.

[7] Ma M, 2020, Corporate Compliance as a Means of Crime Governance. Tribune of Political Science and Law, 2020(3): 168-181.

[8] Zhou Z, 2021, Research on Criminal Law Legislation of Compliance. Criminal Science, 2021(5): 42-54.

[9] Zhao C, 2021, Change in Methods for Identifying Data Crime and Return of Values in the Big-Data Era. Thinking, 2021(5): 140-149.

[10] Yu Z, Li Y, 2014, An Approach to Sanctioning Data Crimes in the Age of Big Data. Social Sciences in China, 2014(10): 100-120, 207.

[11] Yang Z, 2019, Judicial Dilemma and Outlet of Data Crime in China: Focus on the Legal Interests of Data Security. Global Law Review, 2019(6): 151-171.

[12] Chen R, 2020, Compliance Management of Big Data Companies. Chinese Lawyer, 2020(1): 86-88.

[13] Lao D, 2020, Criminal Policy and the Criminal Law System of Functionalism. China Legal Science, 2020(1): 126-148.

[14] Lao D, 2020, The Functional Trend of the Criminal Law System in the Internet Age. China Law Review, 2020(2): 101-114.

[15] Liu X, Shi X, 2021, Construction of Criminal Law Regulation System of Network Data Crime. Research on Rule of Law, 2021(6): 44-55.

[16] Zhou G, 2016, The Establishment of Positive Outlook on Criminal Legislation in China. Chinese Journal of Law, 2016(4): 23-40.

[17] Lang S, 2017, New Development of China's Criminal Law. China Legal Science, 2017(5): 23-46.

[18] Yu C, 2020, Iterative Alienation of Data Security Crimes and the Path to Criminal Law Regulation – From the Perspective of the Introduction of Criminal Compliance Programs. Journal of Northwestern University (Philosophy and Social Sciences Edition), 2020(5): 93-102.

[19] Fu YM, 2021, Legislative Control and Judicial Balance: Criminal Law Amendment Under Positive Outlook on Criminal Law. Contemporary Law Review, 2021(5): 15-27.

[20] Chen R, 2019, Three Dimensions of Corporate Compliance System – Analysis from the Perspective of Comparative Law. Comparative Law Research, 2019(3): 61-77.

[21] Shi Y, 2019, Implementation of Compliance Plan and Criminal Imputation to A Unit. Law Science Magazine, 2019(9): 20-33.

[22] Sun G, 2019, The Concept and Function of Criminal Compliance and the Construction of China. China Criminal Law Journal, 2019(2): 3-24.