Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33399

The Dilemmas of Judicial Application and the Reshaping of Rules in Data Crimes

Qiyan Wang

School of Law, Yangzhou University, Yangzhou, China
3248700499@qq.com

Abstract. In the era of big data, the judicial application of data-related crimes faces two major difficulties. On the one hand, the characterization of such cases tends to expand excessively in a catch-all manner. On the other hand, the criteria for determining the seriousness of crimes remain unclear. The improper use of catch-all provisions, the confusion between different charges and the disconnection of conviction standards have together led to a structural imbalance in the judicial handling of data crimes. These problems stem mainly from outdated theories of legal interests and inadequate regulatory provisions, which have systematically undermined traditional judging standards. To resolve these dilemmas, efforts should be made in two directions. From a judicial perspective, courts should adopt hierarchical interpretation based on layered legal interests, highlight the central position of legal interests concerning data security and establish a hierarchical review rule covering the symbolic level and the content level of data. From a legislative perspective, legislators should improve the legal system through data classification and gradation, add new offenses such as unauthorized use, analysis and possession of data to complete the chain of prohibited conducts and strike a dynamic balance between technological innovation and legal protection.

Keywords: data crimes, judicial application, data legal interests, regulatory framework

1. Introduction

With the rapid growth of the digital economy and the accelerated progress in market based allocation of data elements, data has become the fifth major production factor after land, labor, capital, and technology. The evolution of data boosts people's production efficiency. However, it also brings about a series of issues related to data crimes. In judicial practice, the boundaries between data crimes and offenses such as illegally obtaining data from computer information systems or destroying computer information systems remain unclear. Problems like inconsistent rulings for similar cases and unbalanced standards for crime severity are becoming more prominent.

Data related crimes have become a key topic in criminal law research. Existing discussions mainly focus on two dimensions. The first dimension is institutional construction at the legislative level. It concentrates on macro issues like improving the system of data crime charges and establishing independent legal interests. The second dimension is basic exploration at the level of legal interest theory. It revolves around core concepts such as legal interests in data security and the

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.33399

categorization of data related legal interests. However, existing studies lack in depth examination of the specific application difficulties already emerging in judicial practice. In particular, they fail to systematically address practical problems such as the broadening concept of data and the chaotic application of criminal charges.

Given this, this paper will identify the existing dilemmas in the judicial application of data crimes. It will start from two aspects: the broadening nature of case characterization with unclear boundaries, and the vague standards of crime severity leading to sentencing imbalance. Then it will analyze the causes from two dimensions: the lag in legal interest theory and insufficient normative supply. Finally, it will propose corresponding countermeasures from both judicial and legislative levels.

2. Problem presentation: existing dilemmas in judicial application

China has yet to build a complete and systematic legal norm system for the criminal regulation of data-related crimes. Data infringement acts occur frequently in modern society, and judicial authorities face multiple practical obstacles in relevant law enforcement. For one thing, case conviction shows an obvious trend of generalization. Authorities tend to classify complex data infringement conducts into existing criminal charges in a simplistic manner. For another, clear dividing lines are missing between data crimes and crimes targeting computer information systems. Besides, no unified criteria are available to judge criminalization thresholds and sentencing ranges. These practical bottlenecks greatly hinder the full protection of data rights and interests. Relevant improvements therefore need to be advanced without delay.

2.1. Pocket-like expansion and growing ambiguity in case classification

2.1.1. The crime of illegally obtaining data has become a catch-all provision

The booming development of digital technologies has given rise to numerous new types of crimes. Data is treated as either the object or the essential tool in these emerging illegal acts. In real judicial work high theoretical costs are required to accurately define the legal attributes of relevant targets. Judicial organs therefore often adopt technical attribute evaluation as an alternative judging standard. This change of judging logic brings about a prominent tendency of generalized conviction for the offense of illegally obtaining data from computer information systems [1].Articles 258 and 286 of the Criminal Law of China still place data-related crimes under the regulation system of computer crimes. Rigid legislative positioning restricts proper recognition of data as an independent carrier of legal interests in judicial practice. Explanations of the data concept stay superficial in actual case handling. Genuine protection needs for data rights and interests in the digital age can hardly be satisfied in this way [2].

Popular views in academic circles hold that data only exists as content attached to computer information systems. It represents meaningful combinations of texts symbols sounds images and other materials processed by computer information systems [3]. Such a definition stays restricted to the technology dominated computing-centered computer network era. It thus ignores recognition of the independent value of data itself. Cases including Zheng's illegal [4] acquisition and control of computer information systems and Wang's illegal access to computer information system data [5] fully reveal the technical value and economic value of involved data. These materials also deliver far reaching impacts on personal rights corporate operation and social order in multiple dimensions. Current judicial practice ties data closely to computer information system carriers and applies the

DOI: 10.54254/2753-7048/2026.33399

conviction of illegally obtaining computer information system data. This method can ease the shortage of existing legal norms. It nevertheless conceals the independent legal nature of data and fails to meet the institutional demands for refined protection of data rights and interests across the digital era.

2.1.2. Blurred boundaries between data crimes and crimes of infringing upon citizens' personal information as well as property crimes

With the rapid advancement of network technology today, data grows at an exponential rate. The information it contains is no longer limited to the data itself. Instead, it covers many types of information including personal details and property. This easily blurs the boundaries between concepts like data, personal information, and property. As a result, confusion often arises in judicial practice between data crimes and crimes such as infringing on citizens' personal information or property crimes.

In 2011, the Supreme People's Court and the Supreme People's Procuratorate jointly issued a judicial interpretation. This interpretation concerns the application of law in criminal cases involving harm to computer information system security. It attempts to clarify the scope of application for related charges through restrictive definitions. Specifically, the first two items under paragraph 1 of Article 1 in this interpretation strictly limit the category of data within the crime of illegally obtaining data from computer information systems to identity authentication information.Nevertheless, this restrictive interpretation centers on identity authentication information. Although it aims to separate data crimes from personal information crimes and property crimes, it struggles to keep up with the real world need where data forms become increasingly diverse and data value grows ever richer. On the contrary, it may worsen the classification dilemma faced in judicial application.

Due to the unclear scope and meaning of data, judicial practice often sees inconsistent rulings for similar cases. A typical example is the case of Jiang Honglei and Zhong Chongliang involving illegal acquisition of computer information system data [6]. In this case, the defendant Zhong Chongliang used a password checking tool to clean game accounts. He then discovered that an administrator account for Tencent Company's Xianxian game had the function to generate in game currency called Xianyu. Together with the other defendant Jiang Honglei, he used this administrative authority to illegally generate and transfer game currency for resale and profit. The first instance court convicted him of theft, and the second instance court upheld the ruling. Later, the Liaoning Provincial High People's Court retried the case, overturned the previous rulings, and changed the conviction to illegal acquisition of computer information system data. This back and forth in judicial reasoning deeply exposes a structural flaw in current criminal law regarding data protection. That is, the law focuses on maintaining the functional integrity and security of information systems. At the same time, it emphasizes the privacy protection of personal information. Nevertheless, it fails to pay enough attention to the boundary limits and usability value of data itself. Such imbalance in normative supply makes it difficult for criminal justice to form stable and consistent judgment standards when dealing with the online black and grey industry chain targeting data. Consequently, the practice falls into frequent disputes over case characterization and insufficient regulatory effectiveness [7].

DOI: 10.54254/2753-7048/2026.33399

2.2. Vague quantity standards for crimes lead to imbalanced sentencing

2.2.1. Overly general standards of severe circumstances and serious consequences

Current rules on the quantitative elements of data crimes remain overly abstract and general. Key criteria including severe circumstances and serious consequences lack detailed and targeted design. Existing judicial interpretations set relevant quantitative standards mainly around computer information system security and cyber security. They fail to fully measure the damage inflicted on the legal interest of data security itself. Misaligned evaluation criteria confuse judicial authorities in identifying harmful outcomes. Practical application of criminal charges will also be put in a difficult position as a result [8].

First of all, current quantitative standards make no distinction between different data types and value gaps. Unbalanced sentencing results come into being for this reason. The quantitative evaluation rules formulated by prevailing judicial interpretations show an obvious tendency of simplification. No scientific system of data classification and grading has been adopted as the basic support. The same quantitative criteria are adopted in judicial practice to judge both illegal access to common user accounts and theft of core business confidential data. Huge differences actually exist between the two acts in terms of the depth and scope of damage to legal interests. Such a homogeneous adjudication mode cannot accurately reflect the social harm of different conducts. It also places judicial organs in a tricky situation when judging relevant harmful consequences.

In addition, hierarchical design is missing from current quantitative elements of crimes. The complex forms of data crimes can hardly be well regulated accordingly. Current identification rules for severe circumstances focus merely on single evaluation dimensions such as data quantity and illegal gains. A complete multi dimensional comprehensive evaluation system has not been formed yet. The Data Security Law takes classification and grading systems as the basic arrangement for data governance. It only puts forward differentiated protection requirements for core data important data and general data in principle. Clear classification standards and practical operational guidance are not provided at all. In terms of criminal regulation the graded protection of data under current criminal law remains imperfect. A structural bias of prioritizing data quantity over data quality can be clearly observed [9]. Such misplaced evaluation standards weaken the deterrent effect of criminal law. They also trap judicial authorities in practical dilemmas concerning the selection and application of specific criminal charges.

Lastly, existing quantitative criteria for crimes fail to meet the independent protection needs of data related legal interests. The overall protective effect of legal norms is greatly restricted for this reason. With the in depth development of the digital economy data elements show distinct features of diverse subjects intertwined ownership abundant resources close correlation and growing value. They have evolved into independent production factors and legal interest objects. Their value goes far beyond basic maintenance of system operation. New coverage is expanded to national security public order personal rights and other key fields. Unique legal value independent of traditional technical carriers is fully reflected in modern social progress [10]. Still relevant structural changes are ignored by current judicial interpretations. Legislative lag leaves judicial bodies unable to assess harmful impacts accurately with the help of fixed quantitative rules. Proper implementation of the principle of balanced crime liability and punishment will be hindered in the handling of emerging data infringement acts.

DOI: 10.54254/2753-7048/2026.33399

2.2.2. No matching mechanism between data classification and grading and criminal quantity levels

Article 21 of the Data Security Law establishes a normative framework for data classification and grading. Paragraph 1 lays the institutional foundation. It clarifies the criteria for classification and grading, and it demands the compilation of a catalog of important data for stronger protection. Paragraph 2 defines the scope of core national data, thereby imposing stricter management requirements. Paragraph 3 authorizes regions and industries to formulate their own detailed catalogs. This set of rules offers methodological guidance for criminal justice. That is, only by adopting a differentiated protection strategy based on data type and level can we avoid inefficient resource allocation. Such a strategy applies heavier measures to more critical data and lighter measures to less critical data. In this way, we ensure that key data receives targeted protection [11].

On one hand, the Data Security Law has established a framework and requirements for data classification and grading. However, this framework has not yet been fully or concretely implemented within the criminal justice system. More specifically, relevant institutional designs have failed to turn these requirements into actionable procedural rules and enforcement standards. As a result, their practical application in the criminal justice field faces clear constraints. The normative value of the law thus cannot be effectively released [12]. At present, criminal justice data lacks clear classification and grading standards, along with corresponding differentiated protection measures. This absence makes it difficult for case-handling personnel to follow a unified set of rules during data collection, storage, transmission, and use. Consequently, the boundaries of security responsibility remain vague. Protection priorities are not well defined. This institutional gap directly weakens the capacity for risk identification and prevention. In turn, it becomes a major cause behind the frequent occurrence of data security incidents in criminal justice.

On the other hand, the existing mainstream data classification standards do not align well with China's criminal law system. A considerable number of researchers in the academic circle take personal data, corporate data, and public data as the typological benchmark. They advocate for classification based on ownership [13]. Hence, building a data classification standard that matches the protection goals of criminal law becomes a prerequisite for achieving precise governance of data-related crimes.

3. Cause analysis: the underlying mechanisms of practical dilemmas

The dilemmas existing in the judicial application of data crimes stem from multiple influencing factors. They arise from the intertwined conflicts of legal interest theories normative supply and other realistic conditions. Traditional legal interest theories fail to keep pace with the independent value of emerging data elements. Clear methodological guidance is therefore missing for judicial identification in relevant cases. In addition insufficient right confirmation in preliminary laws and obvious legislative lag bring dual restrictions to data crime governance. Judicial authorities have to adopt extended interpretation to make up for institutional loopholes in regulation.

3.1. Lagging legal interest theory restricts identification approaches

3.1.1. No universal consensus on the independence of data security legal interests

Data has become a core production factor in the digital age. Still wide consensus has not been reached on the independence of data security legal interests in daily judicial practice. The main

DOI: 10.54254/2753-7048/2026.33399

manifestations can be summarized into three aspects.

First, the principle of legal interest protection requires criminal law to offer independent responses to new types of data crimes. Continuous upgrading of digital technology allows data elements to integrate into all fields of social life. Illegal acts such as unauthorized data access malicious data modification data damage and improper data spread occur with growing frequency. They create new protection demands separate from traditional legal interests. Such demands center on the basic safety and core features of data itself. They reflect the need for criminal law to protect data confidentiality integrity and availability [14]. Criminal legislation must grasp the development trend and essential features of new data crimes. These illegal acts come in various forms and spread rapidly. Targeted and forward looking regulatory rules can thus be established for effective governance [15]. The realization of this goal needs clear recognition of the independent status of data security legal interests in criminal law theories. It should no longer be simply attached to traditional legal interests such as computer information system security. Only in this way can the protection needs of legal interests in the digital age be well met.

Second, existing theories fail to fully demonstrate the legitimate basis for protecting the three core attributes of data. Current theories on data security legal interests cannot fully adapt to modern social contexts. They regard confidentiality integrity and availability as inherent natural features of data. Some theories even hold that information forms in the pre digital era shared the same attributes. Such views cannot explain why these attributes receive special protection from criminal law only after the boom of the digital economy. They were not included within the scope of criminal regulation throughout the long historical period before that time. The fundamental reason lies in the lack of a historical perspective in these theories. They only make static summaries of data characteristics and neglect the dynamic formation mechanism of legal interest protection. Clear limitations can be seen in this theoretical framework [16]. Such theoretical flaws weaken the rational support for the independence of data security legal interests. Widespread agreement in academic circles can hardly be achieved as a result.

Third, the legislative tradition of China restricts the independent development of data security legal interests. China's legislation on computer crimes has adopted an integrated framework of equipment computing and data from the very beginning. It centers on computing capacity and covers physical facility dimensions in an implicit way. Less attention has been paid to data elements in comparison. Under this mixed paradigm the independent traits of data crimes and their legal interests fail to gain full recognition [17]. Such reliance on established legislative paths has long kept data regarded as a part of computer information systems or a carrier of information content. It is not treated as an independent object of protection. Faced with the dual predicament of insufficient legislative basis and immature theoretical support the independence of data security legal interests has not been found widely accepted by academic and practical professionals. It eventually turns into a deep rooted barrier blocking the improvement of the data crime governance system.

3.1.2. Absence of a hierarchical review mechanism for data information and systems

Aside from the lack of broad consensus on the independence of data security legal interests as mentioned above, judicial practice has also failed to establish a systematic review mechanism. This leads to two judicial difficulties: vague data concepts and unclear boundaries between data-related crimes.

First, the ambiguity in the path of identifying legal interests stems from the confusion of a three-element relationship. This relationship involves data, information, and the system. In China's criminal law system, judicial practice finds it hard to distinguish the triple nature of data. Data

DOI: 10.54254/2753-7048/2026.33399

serves as an information carrier, as the content of information itself, and as a component of a system. As a result, acts that harm data security get mixed up with acts that damage system functions or violate information content. For example, when someone illegally obtains data stored in a system, current rules do not provide a clear standard for distinguishing the proper evaluation. Should it be seen as an infringement on system security, as a disruption of data management, or as a violation of information content.

Moreover, Second, unclear conceptual boundaries among data, information, and systems further worsen the confusion in judicial determination. Under current criminal law and its judicial interpretations, the definition and connotation of data as a technical concept remain unclear. Its relationship with the two terms information and computer information system is also vague. In some provisions, legislative and judicial authorities treat data and information as equivalent. Yet in other provisions, they confuse data with computer or information systems. This internal contradiction between the two approaches makes it even harder to clarify data's position within criminal law norms [18]. Such conceptual mixing directly leads to difficulty in distinguishing acts that damage computer system functions from those that harm data confidentiality and integrity. Court rulings often base their characterizations on technical appearances rather than on the normative essence.

Finally, the absence of a layered review mechanism also blurs the boundary between data crimes and other types of crimes. In judicial practice, two main interpretive paths exist for applying the offenses that protect data carriers and information content. One path is the integrated interpretation, and the other is the differentiated interpretation. The integrated path tends to cause overprotection of data. The differentiated path, however, may lead to insufficient protection of data. Looking at the root cause, current interpretive paths understand the offenses for criminal law protection of data only from an internal normative perspective. They fail to fully consider external factors related to the norms [19].

3.2. Insufficient norm supply forces judicial overreach

3.2.1. Inherent absence of an independent data crime system

Currently China's criminal law still ties the regulation of data crimes to the traditional system of offences. It has not established an independent and complete set of crime types that match the unique nature of data as a new type of production factor.

Initially, outdated legislative thinking has led to a severe shortage of legal norms. In recent years China has strengthened legal protection for data security. Yet caution still prevails in designing specific constitutions of data-related crimes. In practice the current criminal law mainly relies on traditional offences to govern data crimes. Examples include the crime of illegally obtaining data from a computer information system and the crime of infringing citizens' personal information. No independent and comprehensive crime categories have been created to suit the inherent features of data itself. This legislative approach of using old frameworks to address new challenges fails to adapt to data's unique role as a new production factor. It also cannot effectively cover the risks that may arise at various stages of the entire data life cycle.

Furthermore, chaotic institutional structures leave criminal charge settings without due independence. Up to now, China's Criminal Law has not set a dedicated chapter or section for data crimes and their associated offences. Relevant provisions are scattered across other chapters without systematic institutional arrangements [20].Decentralized legislation results in a vague institutional position for data crimes. Loose logical connections exist among different charges and stop coordinated regulatory effects from taking shape. Meanwhile, the status of data as an independent

DOI: 10.54254/2753-7048/2026.33399

legal interest cannot be highlighted in practice. Existing charge designs still depend on traditional criminal objects and fail to meet the modern demands brought by the market oriented allocation of data elements. Precise protection for the digital economy under criminal law is therefore greatly restricted.

Conclusively, defects in the legislative model hinder independent development. From the perspective of legislative evolution the unified legislative progress of data protection in China has been relatively slow. The legal protection of data rights and personal information has long presented a structural feature of criminal regulation ahead of civil regulation.Back in 2009 the Seventh Criminal Law Amendment created charges such as the crime of selling or illegally providing citizens personal information. Corresponding supporting laws and regulations still failed to be formulated for a long time afterwards. The time difference between advanced criminal legislation and lagging civil legislation leaves the criminal law protection of data without systematic support and coordination from prior laws.For this reason the improvement of legislation on data crimes can only adopt fragmented updates through criminal law amendments. It is difficult to build a systematic and independent normative framework. This situation restricts effective connection between criminal law and prior laws and impedes the modernization of data crime governance [21].

3.2.2. Unclear right confirmation in preceding laws leads to criminal law dependence

Given that preceding laws fail to clearly define data rights, criminal law lacks a solid basis for identifying data legal interests. As a result, it can only rely on the existing normative framework. At present, criminal law does not protect general data on the basis of a full-process preceding legal framework. For this reason, its protection scope remains selective. It mainly focuses on punishing those data violations that cause serious harm to legal interests. This limited protection model directly leads to a fragmented structure within the criminal regulation system for data crimes [22]. Meanwhile, the obligations set by preceding laws appear broad and uncertain. Such vagueness not only erodes the foundation of the principle of legality. It may also improperly expand the scope of criminal liability for internet platforms. What is more serious is that current legislation fails to provide a clear definition of necessary measures. Consequently, platform operators lack clear guidance in their compliance practices. The standards for determining criminal liability or innocence therefore contain significant room for arbitrariness [23]. In this context, improving preceding laws becomes urgent for data crime governance. Clear definitions of data ownership and platform obligations are needed. Only then can a clear normative basis be provided for criminal law application. In turn, this will make data protection and liability determination more law-based and precise.

The absence of preceding laws directly restricts how criminal legislation and judicial practice operate. As for data crimes, the initiation of penal power must be based on a premise. That premise is that the punished act violates a preceding law [24]. It is noteworthy that the involvement of authoritative interpretations or judicial guidance opinions has deeply shaped judicial decision-making practices. Given that preceding laws fail to clarify data ownership, judicial authorities often have no choice but to resort to expansive interpretations. They do so to fill regulatory gaps. This step, in turn, further worsens a certain tendency. That tendency is for data crime determinations to become overly broad and catch-all in nature.

DOI: 10.54254/2753-7048/2026.33399

4. Countermeasure construction two way path of rule restructuring

Practical difficulties persist in the regulation of data crimes. Typical problems include the overuse of generalized conviction vague positioning of legal interests and the absence of clear criteria for sentencing measurement. Systematic rule reshaping is urgently needed from the two dimensions of judicial application and legislative supply.A dual path of rule improvement should be built on judicial theory and legislative theory to break the current deadlock. Layered definition of legal interests will be applied to limit interpretative expansion and boost accurate judicial practice. Meanwhile steady progress in data classification and grading will promote scientific legislative design. A complete criminal regulation system can be established in response to the evolving demands of the digital age.

4.1. Judicial dimension: restricting interpretation through layered legal interests

4.1.1. Establish the core status of data security legal interests

Vague positioning and blurred boundaries still trouble the legal interests protected in data crime regulation. The core status of data security legal interests needs to be confirmed at the normative level. Such a shift will drive the paradigm transformation of data crime identification. It helps move relevant judgment from confusion to accuracy and from passive attachment to full independence.

Data security shall be taken as the core protection legal interest or primary object of data crimes. Clear definition shall be set for the connotation and extension of data crimes. The independence of data security legal interests has remained undetermined. It has led to overlapping norms between data crime judicial identification and property crime or information crime governance. Generalized conviction has appeared frequently in practical operations. Boundaries between different crime types have widened in the blur and the scope of criminal punishment has been expanded in an improper way [25].Judicial application will give full expression to the classification function of data security legal interests in the future. Its independent status and unique connotation will be identified. Data crimes can then be separated from traditional computer crime and information crime systems. Targeted and categorized regulation will be put into practice. The legitimacy and necessity of criminal law intervention can be guaranteed with solid support.

Establishing the core position of data security legal interests is essentially an inevitable choice for criminal law to respond to the needs of the digital era. An independent legal interest system focused on data security can be constructed in this context. It can well resolve normative competition and the improper over expansion of criminal charge application. It also strikes a rational balance between safe data utilization and the protection of individual rights and interests. Firm theoretical foundations are thus laid for the precise and scientific regulation of data related crimes.

4.1.2. Establish layered review rules for symbol layer and content layer

On one hand, a theoretical basis for layered data review should be established. Data crimes can then be refined using Yochai Benkler's three-layer structure theory. The first layer includes the physical layer and the symbol layer. The second layer covers the code layer and the content layer. The third layer is the semantic layer. Under this framework, the physical layer serves as the material foundation for technical implementation. It comprises storage media and hardware devices. The symbol layer acts as the direct object of computer processing. It appears in the form of binary code and data structures. The content layer, in contrast, consists of human-recognizable information with

DOI: 10.54254/2753-7048/2026.33399

practical value. This layer carries specific meanings and social significance. Such a layered review model offers methodological support for clarifying the legal interests protected in data crimes and for distinguishing this offense from others. As a result, it helps make criminal law application more precise and scientific.

On the other hand, a layered interpretation scheme should be introduced. This step avoids either overprotection or underprotection by criminal law. More specifically, drawing on data layering theory, different interpretation paths can be adopted for different dimensions of legal interests. For the symbol layer as data carrier, the focus should fall on its technical security and system integrity. For the content layer as information itself, attention should turn to its social value and ownership of rights. By building differentiated review standards and processing mechanisms, this layered review model can effectively distinguish data infringement acts at different levels.

In summary, we should establish layered review rules for the symbol layer and the content layer. By deconstructing the layered structure of data, these rules enable precise identification of legal interests. They also help draw reasonable boundaries for criminal law. A dynamic balance is thus achieved between ensuring data security and promoting data use. In this way, scientific methodological guidance is provided for the application of criminal law in the digital age.

4.2. Legislative dimension: optimize norm supply via classification and grading

4.2.1. Add crimes of illegal possession illegal use and illegal analysis to complete the conduct chain

China's current criminal law relies on the computer crime system to regulate data crimes. It lacks independently designed criminal charges and breaks the complete regulatory chain. To fix such structural flaws an independent regulatory model matching the inherent features of data should be built through legislation. The whole set of charges shall be improved by covering key links including data acquisition possession use analysis and security protection.

To begin with,a new charge of illegal data possession can be introduced to build a full cycle system for data security protection. This offence targets two major types of conduct. Some actors lawfully hold data in the early stage yet lose their right basis in due course. They refuse to fulfill the obligation of destroying data and keep retaining relevant information. Other actors never obtain legitimate possession authority from the very start. They exceed authorized limits and inappropriately keep data beyond their control [26].The addition of this new charge can fully cover data possession and the performance of data security obligations. It fills the gaps in existing criminal provisions for comprehensive protection across the entire data life cycle.

Furthermore, a new offence of illegal data use should be added to bring data utilization within the scope of criminal regulation.Structural flaws remain in legislative arrangements for the full cycle protection of data crimes. Such loopholes can hardly be remedied through criminal legal theories alone. Upgrading criminal legislation in the vertical dimension serves as the most effective solution.It brings illegal acquisition illegal processing and improper utilization in the data circulation chain under unified regulation. A sound legal interest protection system will be formed to cover the whole data life cycle. Systematic governance of data crimes can be achieved from upstream to downstream links in the industrial chain [27].

In addition, new criminal provisions against illegal data analysis can be added to improve criminal regulation over data analysis activities.

The current criminal law of China may include the offence of illegal data analysis. It targets severe illegal analysis acts that seriously disrupt the management order of data analysis with

DOI: 10.54254/2753-7048/2026.33399

aggravating circumstances.Clear behavioral elements and conviction thresholds shall be defined in relevant legislative design. The formulation respects the core role of data analysis in value transformation amid the big data era. It also delivers targeted criminal law protection for the conversion of data from basic resources to valuable assets. A healthy balance between data security and sound development of the digital economy can be maintained in this way.

4.2.2. Establish a linkage mechanism between data classification grading and crime quantity standards

Current sentencing rules for data crimes lack differentiated considerations. They fail to fully reflect differences in interests and value ranks carried by various data types. Targeted and refined governance requires a linked mechanism combining data classification grading and criminal quantity standards. It helps build a differentiated system of criminal conviction thresholds and realizes dynamic matching between data protection levels and criminal liability.From the perspective of data value the classified and graded protection system set forth in the Data Security Law derives its legal basis from notable differences in interest attributes and value scales among distinct data categories. Legislators allocate varying levels of protection on this basis. Their goal lies in striking a flexible balance between the circulation and sharing of data elements and the safeguard of legal rights and interests [28].Future judicial interpretations need to integrate both subjective and objective grading factors. Differentiated conviction benchmarks should be formulated for diverse data processing behaviors. Common examples include tampering forgery leakage theft and interception.Relatively high conviction thresholds may be set for ordinary data at the basic protection level. Lower criminal standards shall apply to data at higher or the highest protection levels. Such arrangements uphold the fundamental principle of balanced crime and punishment.

One thing to note is that certain grading factors show dynamic change. These factors include the means of harm, the consequences of harm, and the degree of harm. For instance, when data crimes involve different types of legal interests such as national security, social order, public interest, and individual rights of citizens, a cross-over or overlap may occur between protection levels and the thresholds for criminal liability. To tackle this issue, a practical suggestion is to issue guiding opinions on conviction and sentencing. Such opinions would clearly list the specific application standards for various offenses under different classification and grading scenarios. This kind of solution offers frontline case-handling personnel operational and clear guidance. At the same time, it preserves necessary judicial discretion. That discretion is needed to effectively respond to the complex and changing circumstances in practice [29].

5. Conclusion

In the era of big data, solving the practical difficulties in judicial application of data crimes requires a two-pronged governance approach. This approach combines judicial narrowing with legislative improvement. To address current practical problems such as the crime of illegally obtaining computer system data becoming a catch-all provision, and vague sentencing standards leading to imbalanced penalties, a two-way interaction should be used. This interaction pairs the theory of layered legal interests with a classification and grading protection mechanism. By doing so, operational and clear guidance can be provided for judicial decisions. A dynamic balance is thus achieved between data security protection and digital economic development. The whole text follows a logical path. That path is problem presentation, cause analysis, and solution construction. First, the surface-level dilemmas are revealed. These include the expansion of data crimes into

DOI: 10.54254/2753-7048/2026.33399

catch-all applications and the lack of clear sentencing standards. Next, the deeper causes are thoroughly examined. These causes lie in outdated legal interest theory and insufficient normative supply. Finally, two major paths are proposed. One path is a narrow interpretation of legal interests through layering at the judicial theory level. The other path is improving the supply of classification and grading rules at the legislative theory level. As the Data Security Law and the Personal Information Protection Law are more deeply implemented, the governance of data crimes must continuously respond to new challenges brought by technological iteration. In a dynamic balance, data security protection and digital economic development can advance together. This provides solid legal guarantees for building a Digital China.

References

[1] Yang, Z. Q. (2018). Empirical analysis and solutions to the over-expansive application of the crime of illegally obtaining data from computer information systems. Law Review, 6, 165.
[2] Yang, Z. Q. (2019). Judicial dilemmas and outlets of data-related crimes in China: Centered on the legal interest of data security. Global Law Review, 6, 153.
[3] Gao, M. X., & Ma, K. C. (2011). Criminal law. Peking University Press, 536.
[4] (2018). Criminal judgment of Gulou District People's Court of Nanjing city, Jiangsu province (2018) Su 0106 Xing Chu 479.
[5] (n.d.). Typical case 9: Wang's case of illegally obtaining data from computer information systems. Issued by Nanjing Intermediate People's Court of Jiangsu province.
[6] (2017). Criminal retrial judgment of Liaoning Higher People's Court (2017) Liao Xing Zai 9.
[7] Zhang, T. (2022). Risk challenges and concept renewal of data crimes in the digital economy era: Taking data-threatened online illegal industries as observation objects. Legal Forum, 5, 121.
[8] Zhang, Y. (2025). The penalty evaluation model of data classification and grading. Journal of Zhejiang Gongshang University.
[9] Wang, Z. (2024). Research on the specific construction of the criminal law protection system for data classification and grading. Journal of Law Application, 5, 152.
[10] Liu, Y. H. (2024). Research on the criminal guarantee system for security risks in the whole life cycle of data elements: From the perspective of the legal interest of digital economy security. Legal Forum, 1, 39.
[11] Zheng, X. (2021). Research on the classification and grading of criminal judicial data. Journal of National Prosecutors College, 6, 3.
[12] Chen, Y. N. (2026). Research on the classification and grading rules of criminal judicial data and the construction of protection mechanism. Journal of China University of Political Science and Law, 1, 169.
[13] Zhang, B. S. (2023). China's scheme for data confirmation: Research on the classification and grading property right system in the context of factor market. Northern Legal Science, 5, 160.
[14] Zibai, W. (2012). Criminal law in the global risk society and information society. Translated by Zhou, Z. Y., Jiang, S. et al. China Legal Publishing House, 308.
[15] Liu, S. Y. (2022). Typification of data legal interest and construction of criminal law protection system. Chinese Criminal Law Journal, 6, 33.
[16] Liu, X. Q. (2024). Improvement on the construction of the charge system for data crimes. Journal of National Prosecutors College, 3, 26.
[17] Li, Y. L. (2019). Perspective on the normative structure in the network transformation of the crime of sabotaging computer information systems. Legal Forum, 2, 44.
[18] Wang, Q. Y. (2019). Thoughts on criminal regulation of data security crimes under the background of artificial intelligence. Legal Forum, 2, 31.
[19] Liu, R. W., & Wang, G. Z. (2026). On the functionalist interpretation of criminal law protection of data. Journal of Renmin University of China, 1, 80.
[20] Wang, H. M. (2023). Dilemmas and outlets of data crime governance in China. Northern Legal Science, 1, 124.
[21] Wang, H. W. (2021). Comparative investigation and system construction of criminal law protection of data. Comparative Law Review, 5, 135.
[22] Yu, H. S. (2023). Review and prospect of the criminal regulation model of data crimes. Legal Science Magazine, 5, 56.

DOI: 10.54254/2753-7048/2026.33399

[23] Liu, S. Y. (2023). The shift to negative prevention and practical development of the criminal governance logic of data crimes. Contemporary Legal Science, 5, 79.
[24] Li, F. M. (2021). Position choice and realization path of criminal law protection of personal data rights. Studies in Law and Business, 6, 60.
[25] Lu, J. (2025). On the legal interest of data availability status: Construction of independent data protection legal interest and its criminal law expansion—Based on the paradigm of differentiated protection of data and information. Journal of Nanning Normal University (Philosophy and Social Sciences Edition), 6, 78.
[26] Zhang, Y. P. (2023). New model of criminal regulation of data crimes and its legislative construction. Law Journal, 2, 31.
[27] Fang, H. Y. (2023). Concrete investigation and strategy optimization of criminal regulation of data crimes. Ningxia Social Sciences, 3, 78.
[28] Xia, W. (2023). On legislative reshaping of data crimes. Law and Social Development, 4, 173.
[29] Zhang, Y. (2021). Criminal law protection of data security classification and grading. Rule of Law Research, 3, 25.