

The Limits of Criminal Law Protection for Corporate Data Rights in the Context of New Economic Crimes

Yue Tan

Wuhan University School of Law, Hubei, China

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: The development of the digital economy has made data a critical production resource for enterprises. Against this backdrop, new forms of economic crimes have emerged, targeting data and utilizing technology as their tool, resulting in severe violations of corporate data rights. Criminal law serves as the ultimate safeguard for various rights and plays a crucial role in protecting corporate data rights. However, overemphasizing data security measures may hinder data flow and technological innovation. Conversely, it would encourage criminal acts and harm the interests of the enterprise. Therefore, given the specific characteristics of emerging economic crimes, it is essential to clarify the appropriate level of constitutional protection for corporate data rights, analyze existing issues, and propose corresponding recommendations. This approach will ensure adequate protection of corporate data rights while facilitating data circulation and technological innovation, thereby enabling more effective responses to the challenges posed by these new types of economic crimes.

Keywords: New types of economic crimes; Enterprise data rights; Protection under criminal law; Protection limit

Online publication: July 15, 2026

1.Introduction

As digital technology becomes increasingly integrated with the real economy, the value of data is becoming increasingly evident and plays a crucial role in corporate competition. New types of economic crimes leverage big data and artificial intelligence to illegally obtain, utilize, or disclose corporate data. These offenses exhibit high levels of concealment and organized nature, along with extensive social harm, severely infringing upon enterprises' data rights and disrupting the normal functioning of the digital economy market. The criminal law serves as a vital instrument for combating crime and safeguarding society, and should provide comprehensive legal protection for enterprises' data rights. However, due to the restrictive nature of criminal law, the protection it provides is not unlimited and must be confined within reasonable boundaries. In practice, there are issues of either excessive or inadequate handling of such cases. Under these circumstances, determining the appropriate level of criminal penalties for corporate data rights in response to emerging economic crimes, while balancing the interests of both enterprises and the market, is an urgent issue requiring thorough investigation.

2. Defining the boundaries of criminal law protection for corporate data rights in the context of new economic crimes

In the era of emerging economic crimes, the issue of the scope of criminal law protection for corporate data rights primarily concerns which data-related violations warrant criminal penalties and which should be regulated by prior laws such as civil law or administrative law. This essentially involves balancing the principle of restraint and necessity in criminal law. The scope of criminal law protection for corporate data rights should be determined based on the type of data involved, the nature of the conduct, and the degree of harm, neither too broad nor too narrow.

Different types of corporate data require varying levels of protection under criminal law. Corporate data encompasses operational data, technical data, customer data, and other categories, each possessing distinct value and necessitating different degrees of remedial measures in the event of infringement. Consequently, the extent of criminal law protection should correspondingly differ for each type of data. Core technological data represents an enterprise's fundamental competitiveness and involves its trade secrets. If illegally obtained or disclosed, such data can cause irreparable significant losses to the enterprise; therefore, it should be a priority subject of protection under criminal law. General business data inherently possess low economic value and high liquidity; minor infringement cases can be resolved through civil compensation or administrative penalties without requiring application of criminal law^[1].

The nature of the act and the extent of its harm serve as crucial criteria for determining the scope of criminal law protection. In modern economic crimes, violations of corporate data rights primarily involve illegal acquisition, unauthorized use, unlawful disclosure, and illicit trading of corporate data. Criminal law should only impose punishment for acts that seriously endanger society, while no criminal liability shall be pursued for acts with minor circumstances and limited harm^[2]. To determine whether an act constitutes significant harm, a comprehensive assessment should be made based on its mode, consequences, and subjective malice. For instance, utilizing technical means to breach an enterprise's data protection mechanisms and systematically stealing critical corporate information, thereby causing substantial losses to the enterprise's operations, constitutes a serious act that endangers society and shall be subject to criminal penalties. Conversely, the occasional acquisition of a small amount of routine operational information without causing actual harm does not warrant prosecution under criminal law.

3. The imbalance in the scope of criminal law protection for corporate data rights against the background of new types of economic crimes

3.1. Excessive intervention by criminal law hinders data circulation and technological innovation

In certain judicial practices, penalties for violations of corporate data rights are excessively severe, escalating issues that should be resolved under civil or administrative law to criminal proceedings, a practice that contravenes the principle of restraint inherent in criminal law. On one hand, there is excessive protection of publicly disclosed corporate data; in some cases, even minor violations of data management regulations that do not constitute serious offenses are treated as criminal offenses, thereby hindering the normal flow of data. On the other hand, there is excessive criticism of minor data breaches that occur during corporate R&D processes or collaborations with other entities due to insufficient understanding of the specific circumstances, often treating them merely as suspected criminal offenses, a practice that stifles corporate innovation vitality^[3]. In other cases, legitimate use within the

scope of proper authorization was mistakenly deemed illegal acquisition, blurring the line between lawful use and unlawful infringement and excessively expanding the scope of criminal law application.

3.2.The insufficient protection under criminal law makes it difficult to curb new types of data-related crimes

New forms of economic crimes leverage technology as a vehicle, giving rise to ever-increasing methods of infringing upon corporate data rights. However, current criminal law provisions fail to keep pace with these developments, leaving certain emerging forms of infringement inadequately penalized. On one hand, there are legislative gaps in addressing new types of data crimes. For certain offenses involving the use of algorithms or web crawlers to infringe upon corporate data, the absence of specific criminal law provisions makes it difficult to establish liability and impose penalties. On the other hand, the crackdown on chain-style data crimes remains inadequate. In the context of new economic development, corporate data breaches typically span the entire process of “acquisition–processing–trafficking–application.” However, judicial practice often focuses solely on investigating the initial stage of illegal data acquisition while neglecting the regulation of subsequent illegal use and trading activities, thereby failing to effectively disrupt the entire criminal chain. Furthermore, there is a lack of adequate safeguards against indirect infringements of corporate data rights. Certain actions, while not directly stealing corporate data, still interfere with its storage or compromise its integrity. Current criminal law provides limited provisions for such behaviors, making it difficult to effectively protect corporate data security^[4].

3.3.The ambiguity of protection standards leads to confusion in judicial application

Currently, the criminal law provides rather vague provisions regarding corporate data rights and interests, lacking specific standards. This results in inconsistent judicial rulings for cases of the same nature in practice. On one hand, the definitions of “serious circumstances” and “particularly serious circumstances” lack clarity, with varying interpretations across regions and courts regarding the severity of corporate data breaches, leading to disparities in sentencing. On the other hand, the boundaries between corporate data rights, personal information, and public interests are blurred. When corporate data contains personal information, it becomes difficult to identify the key areas protected by criminal law, leading to potential biases, either overemphasizing the protection of corporate data rights at the expense of personal information security, or prioritizing personal information protection to the detriment of corporate data rights^[5].

4.A rational approach to defining the scope of criminal law protection for corporate data rights in the context of emerging economic crimes

4.1.Give priority to the principle of proactive legislation and clarify the supplementary role of criminal law

The protection of corporate data rights must strictly adhere to the fundamental principle of “civil regulation taking precedence, administrative regulation serving as a supplement, and criminal law acting as the ultimate safeguard.” It is essential to fully leverage the preliminary regulatory functions of civil and administrative law in data protection, thereby preventing premature and excessive intervention by criminal law. The civil law is the fundamental legislation governing property and personal relationships among equal parties. When corporate data suffers minor damage, the infringer may be held liable through tort or breach-of-contract remedies,

requiring compensation for losses, mitigation of adverse effects, and restoration of original conditions to promptly mitigate the enterprise's losses. Administrative regulations may employ measures such as ordering rectification, imposing fines, or revoking business licenses to regulate enterprises' data collection, utilization, and circulation activities, thereby preventing data-related violations. For data infringement cases involving minor offenses with limited harm, those that neither significantly adversely affect business operations nor disrupt market competition order, they can be fully addressed through prior legal provisions without resorting to criminal law. The application of criminal law to punish responsible parties should only be considered when such violations pose severe social harm that exceeds the scope of applicable prior laws. For instance, when causing substantial financial losses to enterprises, triggering industry-wide disruptions, or endangering public data security. Furthermore, it is essential to clearly define the transitional mechanisms between criminal law and prior laws, establish specific boundaries for their respective applications, specify under what circumstances prior laws apply and when jurisdiction shifts to criminal law, prevent overlapping enforcement, and ensure that criminal law serves solely as a final safeguard mechanism with precise remedial functions.

4.2.Refine the criminal law protection standards and standardize their judicial application

In response to the current inadequacies in criminal law regarding the protection of corporate data rights and the confusion in its application, it is essential to account for the technical complexity of emerging economic crimes, refine relevant criminal legislation, clarify their constitutive elements and sentencing ranges, thereby providing a solid legal basis for judicial practice. First, it is essential to define what constitutes "serious circumstances" and "particularly serious circumstances," establishing detailed regulations based on the enterprise's various types of data, behavioral patterns, harmful consequences, and subjective intent. This prevents significant variations in case outcomes across courts at different levels and ensures consistent sentencing practices. For example, criteria such as the quantity of critical core technology data obtained, the value of illegally traded data, and the extent of losses incurred by enterprises can be used to determine whether the circumstances constitute 'serious severity,' thereby enhancing the practicality of the assessment. In addition, it is essential to clarify the relationship between corporate data rights, personal information, and public interests. When handling corporate data involving personal information, both corporate data rights must be properly protected, and individual information security must be safeguarded. Neither should the focus be solely on protecting data rights at the expense of personal information rights, nor should excessive emphasis on protecting personal information undermine corporate data rights. For corporate data involving public interests, such as data related to public safety or public services, the extent of its protection under criminal law should be reasonably limited. This approach must balance the protection of corporate interests with the consideration of public welfare needs. Simultaneously, timely judicial interpretations should be issued to address the constantly emerging new types of data crimes, clearly defining the legal penalties for violations such as algorithm abuse or improper use of web scraping technologies that infringe upon corporate data. This will address the shortcomings in existing laws and effectively curb all forms of data crimes.

4.3.Distinguish data types from behavioral characteristics to precisely define protection boundaries

Enterprise data comes in diverse forms and carries varying levels of value, and the methods of data infringement also differ. When defining the boundaries of criminal penalties, the principle of differentiation should be upheld, with the scope of criminal penalties determined based on the specific type of data and the nature of the offense.

Based on an analysis of the value and importance of corporate data, a differentiated approach should be adopted, with varying degrees of protection under criminal law. Critical information vital to an enterprise's survival, such as core confidential data and sensitive operational data, should receive prioritized protection. Infringement of such data would inflict irreparable and substantial losses on the enterprise, necessitating its inclusion within the key regulatory scope of criminal law. For general publicly available data and non-sensitive operational data, information of limited value and high liquidity, protection measures may be appropriately relaxed. Only in cases of severe infringement should criminal law intervention be considered to avoid unnecessary disruptions to normal data flows. At the same time, it is essential to clearly distinguish between lawful utilization and illegal appropriation, and establish clear standards for lawful authorization and fair use. When enterprises engage in activities such as scientific research and development, data sharing, or joint operations, normal usage practices that are legally authorized and comply with relevant industry regulations should not face criminal liability, thereby safeguarding their capacity for technological innovation and their data circulation needs. Those who exceed their authorized authority, employ illegal technical means to breach an enterprise's data defense system, and thereby illegally possess, use, trade, or disclose corporate data shall be held criminally liable in accordance with the law. Furthermore, in response to the industrialized pattern of 'acquisition-processing-transaction-abuse' characteristic of emerging economic crimes, comprehensive efforts have been intensified to combat data-related offenses. While imposing severe penalties for illegal data acquisition at the source, authorities have also stepped up efforts to crack down on subsequent illegal data processing, trading, and misuse, thereby severing the criminal chain and curbing the growth of new data crimes at their root.

4.4.Strengthen the restraint nature of criminal law while balancing technological innovation and data circulation

In protecting corporate data rights under criminal law, it is essential to strictly adhere to the principle of restraint in criminal law application, upholding the philosophy of "avoiding punishment whenever possible and imposing lenient penalties where feasible." This approach prevents excessive interference by criminal law while accommodating technological innovation and the needs of data circulation. The development of the digital economy relies on technological innovation and data circulation. Excessive criminal penalties may dampen enterprises' motivation for technological innovation and hinder the rational allocation of data as a production factor. For routine data-related violations arising from misinterpretation of data scope or improper handling during technological innovation or data research, an approach emphasizing education over punishment should be adopted, through administrative penalties, compliance rectifications, and warning education, to guide enterprises in proper data usage and enhanced data protection measures, without immediate criminal sanctions. Concurrently, clear criminal law boundaries should be established for data circulation, enabling enterprises to engage in data sharing, trading, and collaboration while complying with relevant laws and regulations. This clarifies legitimate data circulation pathways, alleviates corporate concerns, and improves the efficiency of data utilization. By enhancing the restraint of criminal law, we can effectively protect corporate data rights while promoting the coordinated development of technological innovation and data flow. This approach not only upholds the fundamental principles of data security but also fosters a sound legal business environment for the healthy growth of the digital economy.

5. Conclusion

In the context of emerging economic crimes, providing criminal law protection for corporate data rights serves as an effective means to uphold the order of the digital economy and safeguard corporate interests. However, defining its scope appropriately is a prerequisite for achieving dual benefits for both enterprises and the market. Currently, the criminal law protection of corporate data rights suffers from excessive intervention, insufficient safeguards, and ambiguous standards, which hinders data flow and technological advancement. Therefore, the principle of prioritizing civil and administrative measures over criminal penalties should be adhered to. Legislation should further clarify the specific circumstances under which relevant offenses apply and establish corresponding legal regulatory measures tailored to different types of data and conduct patterns, thereby reflecting the restraint and specificity of criminal law and enabling a scientifically sound determination of the extent of protection afforded. This approach not only effectively curbs various emerging forms of data crimes and safeguards enterprises' legitimate rights and interests, but also facilitates data circulation and technological innovation, thereby promoting the healthy development of the digital economy.

Disclosure statement

The author declares no conflict of interest.

References

- [1] Fang H, Location and Path: Identification of Legal Interests and Criminal Law Protection of Platform Data. *Journal of Hebei University (Philosophy and Social Sciences Edition)*, 1–15.
- [2] Fang H, 2025, The Concept, Boundaries and Pathways of Criminal Law Protection for Data Security. *Shandong Social Sciences*, 2025(12): 84–93.
- [3] Fang H, 2025, The Limits of Criminal Law Protection for Corporate Data Rights under the Background of New Economic Crimes. *Journal of Shenzhen University (Humanities and Social Sciences Edition)*, 42(3): 98–107.
- [4] Peng W, 2024, Research on New Types of Crimes and the System of Legal Consequences for Crimes in the Digital Age, China University of Political Science and Law Press, 202406.497.
- [5] Zhao T, 2023, Normative Attributes of Property Data and Criminal Law Protection Strategies. *Lanzhou Academic Journal*, 2023(7): 94–107.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.