Criminal Law Protection Paths for Data Property Rights: A Perspective on Data Theft

Feilin Chen*

Criminal Investigation Police University of China, Shenyang 110854, China

fayleen726@163.com

Abstract. With the rapid development of the digital economy, data has evolved into a key production factor with significant economic value. However, the rise of data theft—characterized by unauthorized access, copying, and transfer—poses substantial challenges to existing criminal law frameworks. Traditional doctrines, primarily designed to protect tangible property or information security, struggle to adequately address infringements upon data-related economic interests.This paper argues that data should be recognized as a form of property interest within criminal law. Despite its intangible and replicable nature, data possesses controllability, transferability, and value-generating capacity, which justify its inclusion as a protected legal interest. On this basis, the paper examines the doctrinal obstacles in regulating data theft, including the incompatibility with traditional theft structures, the limitations of information-related offenses, and the difficulties in loss assessment.To overcome these challenges, this study proposes a systematic protection approach: clarifying the legal status of data property interests, reconstructing the criteria for identifying data theft based on the infringement of control, optimizing the offense structure, and improving methods for evaluating economic loss. These measures aim to establish a coherent criminal law framework capable of effectively addressing data theft in the digital age.

Keywords: Data Property Rights, Digital Economy, Criminal Law Protection.

1 Introduction

In recent years, the rapid expansion of the digital economy has fundamentally reshaped the structure of economic production. Data, once regarded merely as a medium of information, has increasingly assumed the role of a strategic asset. In many sectors, competitive advantage is no longer determined primarily by the ownership of physical resources, but by the capacity to collect, process, and utilize data. As a result, data has come to function as a core factor of production, comparable in significance to capital and technology.

This transformation has been accompanied by a marked increase in unlawful activities involving data. Among these, data theft has emerged as a particularly salient issue. In practice, such conduct typically involves unauthorized access, large-scale copying, and subsequent commercial use of data. [1] Unlike conventional forms of theft,

C. F. Peng et al. (eds.), *Proceedings of the 2026 5th International Conference on Humanities, Wisdom Education and Service Management (HWESM 2026)*, Advances in Social Science, Education and Humanities Research 1024,
https://doi.org/10.2991/978-2-38476-593-5_81

however, data theft does not necessarily entail the physical removal of property. The offender often obtains a copy of the data while the original holder retains access, thereby creating a situation in which appropriation occurs without dispossession. This feature poses a direct challenge to the conceptual framework of criminal law. Traditional doctrines of theft are premised on the idea of exclusive possession and its transfer from one party to another. When applied to data, this logic becomes difficult to sustain. If the victim is not deprived of possession in a tangible sense, it remains unclear whether the conduct can be adequately captured by existing property offenses. The difficulty, therefore, lies not merely in the application of legal rules, but in the adequacy of the underlying concepts themselves.

Current legal responses tend to rely on information-related offenses, particularly those aimed at protecting system security or personal information. While these provisions serve important regulatory purposes, they are not designed to address the economic dimension of data. Consequently, the existing framework places greater emphasis on the protection of informational order than on the safeguarding of data-related property interests. This imbalance has led to fragmented legal approaches and, in some cases, inconsistent judicial outcomes. Against this background, a more fundamental inquiry becomes necessary: should data be recognized as a form of property interest within criminal law, and if so, how should the unlawful appropriation of data be conceptualized and regulated? Addressing this question requires not only doctrinal clarification but also a reconsideration of the basic assumptions underlying property crimes in the digital age.

This paper seeks to contribute to this inquiry by examining the criminal law protection of data property rights from the perspective of data theft. It proceeds in three steps. First, it establishes the theoretical basis for recognizing data as a property interest. Second, it identifies the normative dilemmas that arise in the current legal framework. Third, it proposes a structured approach to reconstructing the criteria and mechanisms for regulating data theft. Through this analysis, the paper aims to provide a more coherent and effective framework for addressing data-related offenses in contemporary criminal law.

2 Theoretical Foundations: The Criminal Law Nature of Data Property Rights

2.1 Justification of Data as a Property Interest

Whether data can be protected under criminal law as a form of property depends, in the first place, on its qualification as a property interest. A purely formal understanding of property, limited to tangible objects, is increasingly unable to account for the transformation of economic relations in the digital age. What is required instead is a functional approach that focuses on the role played by the object in structuring economic interests.

From this perspective, data exhibits several characteristics that justify its classification as a property interest. First, it is subject to effective control. Through technical measures such as access restrictions, encryption, and platform governance mechanisms,

data holders are able to regulate who may access and use data. Although such control is not grounded in physical possession, it nonetheless establishes a form of exclusivity that is functionally comparable to traditional property. Second, data is transferable. It can be licensed, traded, or otherwise monetized through contractual arrangements, demonstrating its integration into market transactions. Third, data has significant economic value. In data-driven markets, the ability to collect and analyze data directly translates into commercial advantage, making data a core asset in modern economic activities.[2] It is true that data differs from traditional property in that it is non-rivalrous and easily replicable.

However, these features do not negate its property character. Rather, they indicate that the mechanisms of protection must be adapted. Replicability does not eliminate economic value; it changes the way in which such value is threatened and appropriated. As long as data embodies economically valuable and controllable interests, it can be recognized as a new type of property interest within criminal law.

2.2 The Structure of Data Property Rights

Once data is recognized as a property interest, it becomes necessary to clarify the internal structure of the rights it entails. Unlike traditional ownership, which is often conceptualized as a unitary and absolute right, data property rights are better understood as a bundle of interrelated entitlements centered on control and exploitation. At the core of this structure is the control right. This refers to the ability of the data holder to determine access to and use of the data. Control is exercised through both technical and legal means, including access permissions, confidentiality agreements, and platform rules. The infringement of this control—through unauthorized access, copying, or dissemination—constitutes the primary form of interference with data property rights.Closely related to control is the use right, which encompasses the ability to exploit data for various purposes, such as analysis, product development, and service provision. In the digital economy, the value of data is realized primarily through its use rather than mere possession.[3] Unauthorized extraction or misuse of data therefore directly undermines the legitimate interests of the data holder. In addition, data property rights include the benefit right, namely the entitlement to derive economic gains from data. These gains may take the form of direct revenues from data transactions or indirect advantages such as improved market positioning and innovation capacity. When data is misappropriated, the harm suffered by the data holder often manifests in the erosion of such benefits, even in the absence of physical deprivation.

Understanding data property rights as a structured set of control, use, and benefit rights makes it possible to more precisely identify the nature of the interests at stake. It also provides an analytical framework for assessing how different forms of data theft interfere with these interests.

2.3 Normative Justification for Criminal Law Protection of Data Property Interests

The recognition of data as a property interest does not automatically entail criminal law protection. Given the principle of restraint, criminal law should be invoked only where other legal mechanisms are insufficient to address serious harm. The question, therefore, is whether the protection of data property interests meets this threshold.

In many cases, civil and administrative remedies prove inadequate. Civil litigation is often hindered by difficulties in evidence collection, high enforcement costs, and limited deterrent effect, particularly in cases involving large-scale or cross-border data misappropriation. Administrative regulation, while capable of imposing compliance obligations, may lack the coercive force necessary to prevent intentional and profit-driven infringements. As a result, reliance solely on non-criminal mechanisms may leave significant gaps in protection. Moreover, the harm caused by data theft frequently extends beyond individual interests. The unauthorized acquisition and exploitation of valuable datasets can distort market competition, undermine trust in digital platforms, and generate substantial economic losses. In such cases, the infringement is not merely private in nature but affects broader economic order, thereby justifying criminal law intervention.[4] At the same time, the extension of criminal law must remain carefully circumscribed. Not all forms of data-related misconduct warrant criminalization. Minor or incidental violations may be more appropriately addressed through civil or administrative measures. The key lies in identifying conduct that seriously interferes with the control and economic interests associated with data, and that cannot be effectively deterred by less intrusive means.

In this sense, the justification for criminal law protection of data property interests rests on a dual consideration: the significance of the interests at stake and the insufficiency of alternative regulatory mechanisms. Where both conditions are met, the involvement of criminal law is not only permissible but necessary. This conclusion provides the normative foundation for examining the shortcomings of the current legal framework and for developing more appropriate regulatory responses to data theft.

3 Normative Dilemmas: Obstacles in the Criminal Law Regulation of Data Theft

3.1 Structural Incompatibility with Traditional Theft Doctrine

A primary obstacle in regulating data theft lies in the structural incompatibility between such conduct and the traditional doctrine of theft. Under classical criminal law theory, theft requires the unlawful taking of another property with the intent of illegal possession, typically resulting in the transfer of possession from the victim to the offender.[5] This doctrinal structure is premised upon the physical nature of property and the exclusivity of possession.

However, data fundamentally challenges this framework. In most cases of data theft, the offender acquires data through copying or downloading, without depriving the original holder of access. The absence of dispossession makes it difficult to satisfy the

requirement of "taking" or "transfer of possession," which has long been considered a core element of theft. As a result, the application of traditional theft provisions to data-related conduct becomes doctrinally strained.

Furthermore, the concept of "illegal possession" is not easily adaptable to data. Since data can be simultaneously possessed by multiple parties, the idea of exclusive possession loses its traditional meaning. Attempts to extend theft doctrine to data through expansive interpretation risk undermining the principle of legality, as they may blur the boundaries between interpretation and analogy. Consequently, the existing framework of theft fails to provide a stable and coherent basis for addressing data theft.

3.2 Functional Deviation and Imbalance in the Existing Offense System

In the absence of a suitable application of traditional theft doctrine, legal practice has turned to information-related offenses as the primary means of regulating data theft. These offenses typically criminalize unauthorized access to computer systems, illegal acquisition of data, and the infringement of personal information. While they play an important role in safeguarding information security and protecting individual privacy, their functional orientation reveals significant limitations when applied to data property interests.

Information-related offenses are primarily designed to protect informational order rather than economic interests. Their focus lies in maintaining the security and integrity of information systems, rather than addressing the economic harm resulting from data misappropriation. As a result, cases involving commercially valuable data may not be adequately captured within their scope, or may be addressed in a manner that underestimates the severity of the harm. The reliance on such offenses has led to an imbalance in the protection of different types of data. Personal data, for instance, is often afforded stronger protection due to its connection with privacy rights, whereas non-personal commercial data may receive comparatively weaker protection. This disparity does not reflect the actual economic significance of different categories of data and may distort legal responses. The lack of a unified framework results in inconsistent judicial application. Similar acts of data theft may be characterized differently depending on the specific circumstances of the case or the interpretive approach of the court. Some cases are treated as violations of information security, while others may be addressed through alternative charges. This inconsistency undermines legal certainty and reduces the predictability of judicial outcomes.

Overall, the current offense system exhibits a functional deviation from the protection of property interests and an imbalance in its application, highlighting the need for a more coherent regulatory approach.

3.3 Normative Difficulties in Evaluating Harm and Loss

Another major challenge in the criminal regulation of data theft concerns the evaluation of harm and the assessment of economic loss. In traditional property crimes, loss is typically measured by the market value of the stolen object or the cost of replacement.

Such methods rely on the assumption that property is tangible, scarce, and subject to exclusive possession. These assumptions, however, do not hold in the context of data.

The value of data is often context-dependent and dynamic. It may vary depending on factors such as the timing of its use, the scope of its application, and the competitive environment in which it is exploited. For example, a dataset may be highly valuable to one enterprise due to its relevance to specific business operations, while having limited value to others. This variability makes it difficult to establish a uniform standard for valuation.

Moreover, the harm caused by data theft is not limited to direct economic loss. Even when the original holder retains access to the data, unauthorized copying may result in the erosion of competitive advantage, loss of exclusivity, and diminished market opportunities. These forms of harm are often indirect and difficult to quantify, yet they may constitute the most significant consequences of data theft. In addition, the diversity of data theft behaviors further complicates the evaluation process. Unauthorized access, large-scale data scraping, internal data leakage, and commercial resale of data may all produce different types and degrees of harm. The absence of clear criteria for distinguishing between these behaviors and assessing their impact leads to uncertainty in determining criminal liability and sentencing.

Taken together, these difficulties indicate that existing methods of evaluating harm are insufficient for addressing the unique characteristics of data. Without a refined framework for assessing loss, the criminal law cannot effectively reflect the seriousness of data theft or ensure proportional punishment.

4 Protection Path: Constructing a Criminal Law Framework for Data Property Rights

4.1 Recognition and Positioning of Data Property Interests in Criminal Law

A prerequisite for the effective regulation of data theft is the explicit recognition of data property interests within the framework of criminal law. As discussed above, data possesses characteristics such as controllability, transferability, and economic value, which justify its classification as a form of property interest. However, the absence of clear legal recognition has led to ambiguity in judicial practice and fragmented application of criminal provisions.

To address this issue, it is necessary to clarify, through legislative interpretation or judicial guidance, that data—particularly commercially valuable data—falls within the scope of protected legal interests in criminal law. Such recognition does not require a rigid assimilation of data into traditional categories of tangible property. Instead, it calls for a functional understanding of property that accommodates new forms of economic resources in the digital age.

At the same time, the positioning of data property interests should reflect a dual-protection approach. On the one hand, data-related offenses often involve threats to informational order, such as breaches of system security or violations of access rules. On the other hand, they may directly infringe upon economic interests associated with data

control and utilization. Therefore, criminal law should integrate both dimensions, recognizing that the protection of data involves not only maintaining order but also safeguarding property interests. This dual orientation provides a more comprehensive foundation for addressing data theft.

4.2 Reconstruction of the Criteria for Identifying Data Theft

The core of reform lies in reconstructing the criteria for identifying data theft in a manner that reflects the unique characteristics of data. The traditional focus on physical dispossession and transfer of possession should be replaced by a more flexible standard centered on the infringement of control.

Under this approach, the key question is whether the offender's conduct has substantially undermined the data holder's control over the data. Control, in this context, refers to the ability to determine access, use, and dissemination of data. When an individual gains unauthorized access to data, copies it, or transfers it to third parties without permission, such conduct interferes with the data holder's exclusive control, even if the original data remains intact. This shift in focus allows for a unified evaluation of various forms of data theft. Unauthorized access, large-scale copying, data scraping, and commercial exploitation can all be assessed under the same conceptual framework, provided that they result in a substantial infringement of control or economic interests. It also avoids the artificial distinction between "taking" and "copying," which has long hindered the application of traditional theft doctrine.

At the same time, the reconstruction of criteria must be accompanied by appropriate limitations to prevent over-criminalization. Not every unauthorized access or minor misuse of data should be treated as criminal. The threshold for criminal liability should be defined by factors such as the scale of the data involved, the intent of the offender, and the extent of harm caused. Only conduct that seriously infringes upon the control and economic interests of the data holder should be subject to criminal sanctions. By adopting the infringement of control as the central standard, criminal law can better capture the essence of data theft and provide a more coherent basis for legal evaluation.

4.3 Coordinated Improvement of the Offense System and Loss Assessment Rules

Beyond redefining data theft, it is necessary to refine both the structure of criminal offenses and methods of loss assessment, as offense classification depends on the nature and extent of harm. The relationship between traditional property crimes and information-related offenses should be coordinated by distinguishing data-related conduct based on the primary interest affected. [6] Conduct undermining informational order should fall under information-related offenses, while conduct harming economic interests in data should be addressed through property-based approaches, enhancing precision and consistency.

In the long term, a distinct category of data-related property crimes could be established to better define offenses and protected interests while preserving legality. Loss assessment should adopt a multi-dimensional approach, considering market value,

development cost, and economic benefits, as well as competitive harm such as loss of market advantage. It should also account for indirect and long-term impacts. A more flexible valuation framework would improve the accuracy of harm assessment and ensure proportionate punishment, thereby strengthening criminal law protection of data property rights in the digital economy.

5 Conclusion

The digital economy has revealed the limits of traditional criminal law in addressing data theft. As data functions as a form of property with economic value and controllability, criminal law protection is justified where serious harm and regulatory gaps exist. Yet current frameworks remain fragmented, due to tensions with traditional theft doctrine, misaligned offense structures, and difficulties in assessing loss.

This paper argues for a shift toward a control- and interest-based approach. By recognizing data property interests, redefining the criteria of data theft, and improving offense classification and loss assessment, a more coherent and effective legal framework can be established. Such reform would enhance legal certainty and ensure proportionate responses to data-related crimes in the digital age.

References

1. E.Stefan Kehlenbach.: Data dispossession: against the property model of data. Contemporary Political Theory24(4):1-19(2025).
2. Xiong, B.: The independent construction of data property and its criminal law protection. Oriental Law, (6), 47–66(2025).
3. Myra F. Din.: Breaching and Entering: When Data Scraping Should be a Federal Computer Hacking Crime . Brooklyn Law Review. 81: 418(2015).
4. Andrew Sellars.: Twenty Years of Web Scraping and the Computer Fraud and Abuse Act . Boston University Journal of Science and Technology Law. 24: 394(2018).
5. Li, T., & Chi, Y.: Legal dilemmas and multi-dimensional governance mechanisms for shared data privacy protection. Journal of Hunan Agricultural University (Social Sciences), 27(2), 69–77(2026).
6. Wang, L.: Criminal law protection of enterprise data properization. Legal Forum, 41(1), 90–101(2026).