The Legal Implementation of the Security of Enterprise Data Assets

Fei Teng
School of Law, China Jiliang University, Hangzhou, Zhejiang, China

Abstract: As a novel form of collateral in the digital economy era, the security of enterprise data assets represents a key institutional innovation to promote the capitalization of data elements. Enterprise data assets, being intangible properties, have exchange values that meet the core criteria for eligible collateral, thus enabling the establishment of security. The legal characteristics of enterprise data assets and the structure of right pledges determine that creating a right pledge thereon is more appropriate than establishing a mortgage. The security of enterprise data assets can, based on the fundamental principles of security, reference the pledge method, rely on a national integrated data registration authority, and implement a registration-effective model. Meanwhile, it is necessary to establish and improve the basic legal system for data asset pledges, introduce licensing use as the means to enforce enterprise data asset security, optimize the security enforcement path by integrating smart contract technology, and effectively safeguard the valid exercise of data asset pledge rights.

Keywords: Data Asset Security; Secured Property; Pledge of Rights; Registration Effectiveness

1. Introduction

"Data is the oil of the new era" – since mathematician Clive Humby proposed this view in 2006, the value creation mechanism of data elements has gradually completed a three-stage evolution: resourceization sedimentation, assetization transformation, and capitalization leap. In the digital economic society, data assets have not only become the core resources of enterprises, but also serve as an engine driving business model innovation and value creation, while enabling cross-domain circulation of basic social resources in their morphological form.

The attributes of enterprise data assets have gradually become prominent. In the commercial utilization of data, there are increasingly rich practical cases where enterprises use data assets for financing security. The expression of "financing security" reflects the practical significance of the security system – it is an institutional supply that enhances the debtor's credit and ensures the smooth realization of creditor's rights by designating enterprise data assets as legitimate collateral, thus meeting the financing needs of transaction subjects. This represents a positive response by law, guided by the reflexive paradigm, to the current new risk society context. However, China's existing laws and administrative regulations have not explicitly stipulated the security of enterprise data assets, leaving this innovative financing model on the fringes of the law and constituting a hindrance to the development of enterprise data asset financing security business. Facing the economic demand for enterprise data assets as financing security tools, there is an urgent need for legal response. Therefore, this paper explores the feasibility of incorporating emerging data assets into the traditional security system and clarifies the path for security realization. This is not only of great significance for the development of the data trading market and the improvement of data asset theory, but also an important mission to boost digital economic development and the market-oriented allocation of data elements through financial rule of law.

2. Legal Attributes of Corporate Data Assets and Their Viability as Security Property

2.1 Analysis of Legal Attributes of Corporate Data Assets

Corporate data assets are not an inherent concept in current legislation. The term "data asset" originates primarily from normative documents rather than arbitrary phrasing. Certain normative instruments define corporate data assets from an accounting perspective as "data resources lawfully owned or controlled by a specific entity, capable of monetary measurement, and able to generate economic or social benefits." The definition of data assets carries the following legal implications: first, it does not require the establishment of data asset ownership; legal control alone suffices to establish entitlement. Second, data assets encompass a broad scope, and there is no requirement to form structured databases through processing. Third, data assets are characterized by utility, with their economic or social benefits realized through measurement or transactions. By adopting "legal control" as the core ownership requirement, this definition circumvents debates over data ownership [1]. Through accounting recognition, it clarifies the legitimacy of an enterprise's property rights over data assets, thereby laying a legal foundation for subsequent secured transactions involving such assets.

From an accounting perspective, explaining the concept and scope of data assets fails to accurately summarize and extract the theoretical nature and legal characteristics of data assets. Therefore, defining its basic connotation from a legal perspective is a prerequisite for solving the problem of enterprise data asset security. Enterprise data assets are intangible properties. Traditional legislation generally does not distinguish between things and properties. Although China's Civil Code sometimes confuses things with properties, it emphasizes that any object with value attributes can be called property. Properties are divided into tangible and intangible properties according to their physical forms. Intangible properties are recognized in China's legislation and judicature, such as patent rights. The primary value goal of the property system is to define the rights boundaries of transaction subjects, thereby forming properties belonging to the subjects [2]. Therefore, as intangible properties, enterprise data assets are essentially a kind of right [3], which refers to both the data resources with transaction value held or controlled by enterprises in the production and operation process and the rights enjoyed by enterprises over such data assets, providing a theoretical basis for Pledge of rights.

Enterprise data assets have the following particularities compared with traditional secured properties: first, non-physicality, existing in binary code without physical loss; second, value dynamics and scenario dependency, featuring "increasing returns to scale" with different valuations in different scenarios, leading to valuation difficulties; third, reproducibility, where copied data remains identical to the original and can be simultaneously controlled by both the security provider and the secured party, which does not contradict the exclusivity in the value judgment dimension.

2.2 Legality of Enterprise Data Assets as Security Properties

Enterprise data assets possess both practical necessity and legal eligibility as security properties. In terms of practical needs, they serve as a crucial support for the data transaction system, forming the institutional cornerstone of the data transaction safety net through their risk mitigation function. Meanwhile, as a new form of data economy, they can address the light-asset financing challenges of technology-based small and medium-sized enterprises, promote the capital conversion of data elements, and facilitate the digital transformation of real industries. In practice, financial institutions have already launched relevant secured transactions involving data assets.

In terms of legality, according to the traditional continental civil law theory of security real rights, the essence of security interests lies in the right of realization – the right holder disposes of the security object and realizes the principal claim from the proceeds of liquidation [4]. Therefore, the core lies in the justification of the exchange value of the security object. Enterprise data assets, having been processed to embody human labor, conform to Locke's labor theory of property, and policies such as the Data Twenty Articles explicitly recognize their property value. In practice, they possess the capacity for market circulation and monetization.

The dominium of enterprises over data assets is achieved through technical control and legal frameworks, with its legitimacy deriving from value-added labor and the "right separation" from personal information. The exclusivity of enterprise data assets is manifested as limited exclusivity protected by laws such as the Civil Code at the regulatory level, and their specificity can be realized through technical sealing and access control, which meets the eligibility criteria for collateral property. Variables such as the current operation of data trading markets only serve as risk factors that may affect the enforcement of security rights after the establishment of enterprise data asset security, and cannot constitute grounds for negating the establishment of such security. As intangible properties under the dominium of enterprises, featuring scarcity, transferable property value, as well as legal exclusivity and specificity, enterprise data assets are eligible collateral property.

3. Determination of the Security Type for Enterprise Data Assets

After confirming the eligibility of enterprise data assets as collateral, it is necessary to further clarify the specific type of security to be established.

3.1 Empirical Investigation into Security Types for Enterprise Data Assets

First, regarding the practical manifestations of security types, current pilot scenarios across China have primarily developed two models for enterprise data asset security: (1) Data Asset Mortgage. In April 2016, China's first "data loan" was issued by Guiyang Bank to Guizhou Oriental Century Technology Co., Ltd. using its data assets as mortgage collateral for 1 million RMB; in August 2024, Chongqing Liangjiang Smart City Investment & Development Co., Ltd. obtained Sichuan Province's first 5 million RMB data asset mortgage loan through online registration at the Western Data Exchange; in September 2024, Chongqing Fudimai Digital Technology Co., Ltd. secured Chongqing Municipality's first 5 million RMB data asset mortgage loan from the Chongqing High-Tech Branch of Agricultural Bank of China; in April 2025, Shandong Port Connect Co., Ltd. received Shandong Province's first 5 million RMB data asset mortgage loan. (2) Data Asset Pledge. In September 2021, Zhejiang Fanjv Technology Co., Ltd. completed Zhejiang Province's first 1 million RMB data asset pledge financing with the Binjiang Sub-branch of Shanghai Bank using data-related intellectual property rights; in October 2022, Jiahua Technology Co., Ltd. obtained Beijing Municipality's first 10 million RMB data asset pledge loan from the Sub-center Branch of Beijing Bank; in March 2024, Jiangxi Yingshi Information Engineering Co., Ltd. secured Jiangxi Province's first 5 million RMB full-chain notarized data asset pledge financing from Shangrao Bank; in June 2024, Digital China Holdings Ltd. included its financial cloud data products as data assets in corporate financial statements and received Shenzhen's first 30 million RMB data asset pledge financing from the Shenzhen Branch of China Construction Bank. This coexistence of mortgage and pledge practices demonstrates the current ambiguity in legal classification, leading to inconsistent security methods in practice.

Second, at the regulatory level, there are discrepancies in terminology across regional regulations regarding data asset security transactions. For example, the Interim Measures for the Registration and Management of Data Property Rights in Shenzhen issued by the Shenzhen Municipal Development and Reform Commission defines data asset financing security as a "mortgage", while the Regulations of Guizhou Province on Promoting Data Circulation and Transactions uses the term "pledge" to describe data assets eligible for financing security.

Overall, the authority and standardization of China's enterprise data asset security rules remain insufficient. Market entities lack unified legal basis for autonomously determining security types, which, while pragmatically justifiable during the exploratory innovation phase, have increasingly constrained the standardized operation of data asset financing as the national data element market deepens. Despite ongoing debates on the specific implementation path for data asset security, it is undeniable that the normative logic of the existing civil security system can still provide legal responses, and legal basis can be sought within the established institutional framework.

3.2 Selection of Security Type for Enterprise Data Assets: Pledge of Rights

Academic debates on the security type of enterprise data assets focus on the fundamental opposition between the "mortgage theory" and the "pledge theory". Scholars advocating the mortgage theory cite Article 395 of the Civil Code, arguing that data assets fall under "other properties not prohibited by law," and should be analogized to real estate mortgage rules, with public notice through a registration opposition system while retaining the usufruct of the pledgor [5]. Proponents of the pledge theory, however, expand the interpretation of Paragraph 7, Article 440 of the Civil Code to include data assets within the scope of pledge of rights objects. The registration-based public notice method of pledge of rights aligns with China's ongoing establishment of a unified rights registration and public notice system. Pledge of rights is superior to the data asset mortgage model in terms of object inclusiveness, institutional adaptability, and practical feasibility, better conforming to the reform direction of market-oriented allocation of data elements [6]. This paper argues that pledge of rights has more sufficient jurisprudential basis and higher feasibility in systemic positioning.

From a jurisprudential perspective, as intangible property rights, the legal attributes of enterprise data assets determine that they are more compatible with pledge of rights than right mortgages in security type selection. Enterprise data assets do not meet the object requirements for right mortgages under Article 395 of the Civil Code: they are neither usufructuary rights over real estate nor quasi-property rights, thus cannot be included in the mortgage category. On the contrary, they conform to the core element of “transferable property rights” in Item 7 of Article 440. As data resources legitimately controlled by enterprises with transaction value, they possess the “transferability” required by pledge of rights and can be included in the scope of pledge of rights objects through the omnibus clause.

The historical evolution of the system shows that the scope of pledge of rights objects has always followed the logic of “expansive development,” gradually expanding from early property right certificates such as warehouse receipts and bills of lading to new-type intangible properties like intellectual property rights and equity. This evolutionary path provides an institutional precedent for incorporating enterprise data assets into pledge of rights: both take non-physical property rights as objects and rely on registration public notice rather than physical possession to achieve right control, conforming to the development law of modern security systems adapting to new property forms. In traditional civil law systems, right mortgages are strictly limited to usufructuary rights over real estate, with their institutional design premised on “registration public notice + value stability.” Forcing data assets to analogize real estate mortgage rules and adopting the registration opposition doctrine would trigger inherent conflicts in the public notice mechanism. Movable property mortgages use “possession” as a natural public notice means, but the non-physical nature of data assets makes them inapplicable to physical possession rules, unnecessarily increasing transaction costs and legal risks.

In the security enforcement mechanism, the core difference between mortgage and pledge of rights highlights the superiority of pledge for data assets. A mortgage only requires control over exchange value without transferring possession, and its operation relies on the stability of the collateral’s value and the consistency of the parties’ value expectations. However, the value of data assets is highly dynamic and context-dependent, making mortgage enforcement risky in value realization—it is difficult for the two parties in the security legal relationship to reach a consistent expectation of the data assets’ future exchange value. In contrast, when the debtor fails to perform matured obligations or circumstances for enforcing security rights as agreed occur, the pledgee can directly dispose of the collateral and receive priority compensation from the proceeds. If a mortgagee fails to agree with the mortgagor on the method for enforcing the mortgage, they can only exercise their rights by applying to the court for auction or sale of the collateral. Pledge of rights provides a more direct and convenient relief path for right holders.

In summary, whether from the perspective of jurisprudential adaptability, institutional evolutionary logic, or practical right enforcement efficiency, incorporating enterprise data assets into the category of pledge of rights has a more solid theoretical foundation and practical rationality.

4. Institutional Improvement for Realizing Enterprise Data Asset Security

China’s enterprise data asset security financing mechanism is still in the exploratory stage, currently focusing more on theoretical research and pilot practices. Although the pledge nature of enterprise data asset security can directly apply the general provisions on pledge of rights in the Civil Code, key links such as public notice methods, validity determination, registration authorities, and enforcement paths for data asset pledges lack clear legal definition, urgently requiring improvement of practical norms. In view of this, this paper puts forward targeted suggestions for the implementation of the enterprise data asset pledge mechanism to fill the gaps in the current system.

4.1 Clarifying Public Notice Effect and Registration Rules

4.1.1 Public notice effect of enterprise data asset security: registration for validity

The public notice system in civil law serves both the functions of right establishment and granting rights external effect. It is an institutional manifestation of resolving factual right conflicts and a prerequisite for the principle of party autonomy. Registration is essentially a process recognizable to the outside world, aimed at safeguarding the interests of third parties and transaction security [7]. Under the Civil Code system, the public notice method for movable property mortgages is registration, and pledge of rights also generally adopts registration for public notice. Adopting registration for public notice of data asset security is an act of systemic coherence. Compared with other public notice methods, registration undoubtedly has a stronger public notice effect, which is more conducive to maintaining transaction security. Due to the intangible, reproducible, and highly technical architecture-dependent nature of enterprise data assets, information related to their ownership, scope, status, etc., is mainly stored in electronic registration systems or specific technical platforms, making it impossible to achieve effective public notice through physical possession or delivery of traditional right certificates. Therefore, to ensure transaction security and avoid unnecessary disputes, registration public notice should become the token for establishing and publicizing whether pledge of rights is set on enterprise data assets.

Regarding the effect of public notice, there are mainly the registration-for-validity model and the registration-for-opposability model. The registration-for-validity model has three institutional advantages in enterprise data asset pledges: First, in view of the dynamic characteristics of enterprise data assets, the registration-for-validity model can ensure data quality and prevent product quality liabilities and breach of contract liabilities for data assets; Second, statutory registration grants transaction public trust, which not only reduces the information cost for transaction counterparts to query the ownership status of data, thereby ensuring the public trust of registration and enhancing transaction confidence; Third, addressing the current situation of China’s data market where “on-exchange scale is small and over-the-counter trading is non-standard,” the registration-for-validity model guides decentralized over-the-counter transactions to concentrate in compliant on-exchange markets through a mandatory public notice mechanism. This can both break “data silos” to promote circulation and balance transaction security with market vitality through unified rules, promoting the healthy development of market-oriented allocation of data elements.

The reason for adopting the registration-for-validity model rather than the registration-for-opposability model lies in the risk of hidden security caused by the reproducibility and non-rivalry of enterprise data assets. The registration-for-opposability model cannot fully avoid such risks, while the registration-for-validity model can better eliminate hidden security and balance the interests of security right holders and potential transaction counterparts [8]. Therefore, comparatively speaking, adopting the registration-for-validity model is a better choice to achieve the public notice purpose of enterprise data asset security, that is, enterprise data asset security is established upon registration.

4.1.2 Registration authority for enterprise data asset security

Regarding the registration authority, the current practice of enterprise data asset security transactions lacks a unified national registration authority. Existing security registrations are scattered across local data asset registration platforms and local data exchanges, with local registration authorities appearing fragmented and lacking effective information interoperability and linkage mechanisms between different registration systems. From the perspective of current data property rights registration practices, regions such as Zhejiang Province and Beijing show a tendency to include data pledge registration in intellectual property rights registration. As previously mentioned, intellectual property protection is only an expedient measure in the absence of a specialized data asset protection system, which has limitations for the long-term development of data assets. From the perspective of comprehensive protection, establishing a specialized data property rights registration system is a better choice. Based on the intangible, non-rivalrous, and reproducible characteristics of data assets, an efficient, fair, secure, and controllable data element market cannot be formed without a clear data property rights system defining ownership [9]. Therefore, the core of data protection and utilization lies in establishing a data property rights system that clarifies data ownership. As the saying goes, “where there is a source for the registration and public notice of ownership, that source can serve as the destination for warning registration and public notice” [10].

This paper proposes designating the National Data Bureau-which is responsible for promoting the construction of data basic systems and coordinating data integration and development and utilization – as the authoritative registration authority for data property rights registration and data asset pledge registration. It should establish a unified data property rights registration and public notice system based on internet platforms, providing the public with data property rights registration, data asset pledge registration, and inquiry services.

4.2 Specific Measures to Strengthen the Enforcement of Enterprise Data Asset Security

The traditional enforcement method of security rights centers on the sale of collateral, discharging claims through one-time liquidation of exchange value. Its efficiency relies on the market liquidity and standardization of the collateral, making it more suitable for tangible properties. However, the non-physical, reproducible, and dynamically valued nature of data assets renders them difficult to adapt to traditional liquidation models, thus urgently requiring exploration of usufruct value enforcement methods consistent with the legal characteristics of enterprise data assets. Traditional security enforcement takes right transfer as a precondition, where the right holder loses the actual use qualification of enterprise data assets during enforcement; yet data assets can unleash value potential through multiple development paths and often constitute the core assets and market competitiveness foundation of the security provider, making it necessary to construct an enforcement mechanism that does not transfer data rights.

Future data legislation may consider designating licensing use as the enforcement method for data security rights, where the right holder obtains consideration by authorizing others to use the data. This model is analogous to the rental mechanism of tangible properties, which can fully unleash the multiple values of data while preventing the security provider from losing core assets due to right transfer, thus balancing the interests of both parties in the security relationship. From the perspective of legal interpretation, data licensing use can reference the compulsory management measures stipulated in the Civil Enforcement Law (Draft), combined with adaptive adjustments based on data technical characteristics – for example, achieving precise control over data use through open API interfaces [11].

Smart contract technology can serve as an auxiliary means to enforce security, realizing value transfer through a decentralized mandatory performance mechanism. That is, smart contracts can meet the parties’ trust needs without relying on authoritative third parties, thereby significantly improving transaction efficiency and reducing transaction costs, which aligns with the value orientation of security enforcement [12]. In the event of default by the pledgor, smart contracts can be combined with a reasonable data pricing mechanism to dispose of the collateral at a determined fair price. Their program control avoids the moral hazard of the security provider maliciously disposing of the collateral. Compared with traditional methods, this approach recovers debts more efficiently and at lower cost, enables self-help relief within a compliance framework, saves judicial resources, and lays a foundation for the smooth enforcement of security interests.

5. Conclusion

The enterprise data asset security system serves as the legal key to unlocking the channel of data capitalization. The transformation from “data resources” to “security assets” not only activates the economic potential of data elements but also provides an innovative path to solve the financing dilemma of technology-based enterprises. Under the framework of the enterprise data asset security system, allowing data assets to be used as collateral can unleash the potential of data elements, empower real economy financing, establish a new security model driven by data elements, promote the transformation of financial service forms, and facilitate the healthy development of the digital economy. However, enterprise data assets involve multiple and complex interest relationships, including data right attribution, the interests of security right holders, and data security protection. Therefore, the system design must focus on balancing the internal structure of data rights, the interests of subjects both within and outside the security legal relationship, and data security compliance. With the deepened development of the national integrated data market, data asset security will become an important engine driving the high-quality development of the digital economy, promoting the efficient operation of the "data-asset-capital" value closed loop on the track of the rule of law.

References

[1] Lin Yanzuo. Research on the Rules of Data Asset Security in the Context of Digital Economy. Journal of China University of Mining and Technology (Social Sciences Edition), 2023, 25(5): 89-106.

[2] Peng Chengxin, Gong Sihan. Theoretical Clarification and Normative Construction of Public Data Asset Pledge. Law Journal, 2024, 45(5): 36-52+2.

[3] Ma Junju, Mei Xiaying. The Theory and Legislative Issues of Intangible Property. China Legal Science, 2001, (2): 103-112.

[4] Iesato Wataru. Newly Revised Security Real Rights Law. Beijing: China Legal System Press, 2008.

[5] Zhang Zhengzhang, Chen Shuting. The Justification and Rule Construction of Data Property Rights Security. Journal of Shandong University (Philosophy and Social Sciences Edition), 2025, (2): 175-184.

[6] Song Yunting. On the Collateralizability of Enterprise Data Interests. Financial Development Research, 2024, (3): 64-75.

[7] Yan Wei. The Public Notice Effect of Property Rights Registration and Its Impact on Administrative Actions. China Journal of Applied Law, 2025, (1): 152-167.

[8] Gao Shengping. The Construction of a Unified Movable and Rights Security Registration System from the Perspective of the Civil Code. Journal of Zhejiang Gongshang University, 2020, (5): 38-52.

[9] Wang Chunhui, Fang Xingdong. The Core Essentials of Constructing a Data Property Rights System. Journal of Nanjing University of Posts and Telecommunications (Social Sciences Edition), 2023, 25(1): 19-32.

[10] Dong Xueli. China Should Establish a "Super Unified" Warning Registration and Public Notice System for Security Interests. Legal Forum, 2023, 38(1): 131-138.

[11] Tao Xinming. The Legal Structure of Data Security. Journal of Jiangxi University of Finance and Economics, 2025, (05): 1-17.

[12] Cheng Le. The Construction Path of Smart Contract Clauses under the Double-Layer Structure. Legal Review, 2022, 40(2): 53-66.