Proceedings of the 4th International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.30987

The Rights Foundation and Legal Confirmation of Data Pledge from the Perspective of Rights Decomposition

Jiayi Wang

School of Law and Economics, Zhongnan University of Economics and Law-Sapienza University of Rome, Wuhan, China
wangjiayi558@163.com

Abstract. The legitimacy dilemma of data asset pledge financing stems from the contradiction between the inherent characteristics of data rights themselves and traditional security interest theory. There exists a fundamental contradiction between the non-excludability and replicability of data as an intangible asset and the specificity and exclusivity required by security interests in property rights. This requires breaking through the perspective of rights integrity and adopting a path of rights decomposition, viewing the bundle of data rights as a separable set of sub-rights, namely: data resource holding rights, processing and use rights, and product operation rights. The data processing and use rights, due to their direct control and benefit capacity over data value, can be analogized as a new type of property usufruct right based on the usufruct principle of Article 323 of the Civil Code, thus satisfying the object requirements of security interests in property. Through registration and publicity mechanisms, such as blockchain evidence preservation technology, precise description and boundary fixation of sub-rights can be achieved, realizing the specification of rights and conforming to the principle of specificity of property right objects under Article 114 of the Civil Code. Accordingly, data sub-rights can be incorporated into "other property rights that may be pledged as stipulated by laws and administrative regulations" as provided in Article 440 of the Civil Code, thereby demonstrating the pledge eligibility of data sub-rights.

Keywords: Data asset capitalization, private enterprises, pledge financing, registration and publicity

1. Introduction

Data-backed financing holds the potential to unleash the value of enterprise data while broadening access to funding channels. However, in practice, its legal framework is still plagued by numerous uncertainties. The distinctive characteristics of data as an intangible asset—marked by its non-exclusive nature and ability to be replicated—clash considerably with the specific object requirements and exclusivity embedded in traditional security interest frameworks This tension creates practical challenges, such as formal distortions and ambiguous legal interpretations of data security arrangements. This systemic dilemma not only impacts the efficiency of market-driven

DOI: 10.54254/2753-7048/2025.30987

allocation of data elements but also has the potential to increase transaction risks and result in a rise in legal disputes.

Recent studies on data security challenges predominantly focus on the enhancement and deployment of traditional security frameworks. Certain scholars have sought to establish mortgage rights through a mortgage framework, treating data as intangible assets and utilizing registration and publicity systems. Other research backs a pledge-based strategy, which mimics the transfer of ownership by managing control over data access rights. However, each of these interpretive methods encounters certain limitations. The mortgage method faces difficulties in tackling the insufficient specificity of objects within the data, while the pledge method finds it hard to establish genuine exclusive control. More crucially, current research frequently regards data rights as an indivisible whole, overlooking the autonomy and separability of various sub-rights within the spectrum of data rights. This lack of oversight leads to security measures failing to precisely match the methods for realizing data value.

The central question explored in this paper is how to construct a theoretical framework for data security that aligns with the intrinsic nature of data while complying with legal principles. This framework seeks to resolve the jurisprudential conflict between the non-exclusive nature of data and the exclusive demands of security, providing practical institutional support for the enforcement of data security. To address this question, the paper suggests examining the issue by breaking down rights into their constituent parts. It divides data rights into sub-categories, such as resource holding rights, processing and usage rights, and product operation rights.Special attention is given to exploring whether data processing and usage rights can qualify as independent security objects and investigating the legal avenues for their realization.

2. The legal nature of data asset security

2.1. The phenomenon of formal transformation in security practice

Data asset security in practice has deviated from traditional security forms, with this formal transformation primarily manifested in the non-typicality of security methods and the ambiguity of legal characterization. Under the traditional security interest system, pledge or mortgage generally takes tangible property or clearly defined intangible rights as the object, and requires the realization of security effectiveness through possession transfer or registration publicity. However, in data asset security practice, creditors often indirectly achieve security purposes by controlling data accounts, restricting data access rights, or allocating data usage benefits, rather than directly pledging data rights [1]. This transformation phenomenon is caused by the characteristics of data assets themselves —intangibility, replicability, and non-excludability make traditional security models directly inapplicable. In practice, some transactions use data storage devices or server pledges in name while exercising data control in reality, thereby making the legal nature of security more ambiguous [2]. This transformation leads to disputes over the priority of repayment effectiveness of data security rights in bankruptcy liquidation or execution procedures due to unclear forms.

2.2. The legal conflict between data non-excludability and security excludability

The deep legal conflict between the non-excludability of data assets and the excludability required by security interests in property is the core reason for the ambiguous legal nature of data security. Non-excludability means that the same data can be simultaneously used, processed, or benefited from by multiple parties without diminishing its value or function, forming a sharp contrast with the

DOI: 10.54254/2753-7048/2025.30987

excludability requirements of traditional security interests [3]. Security interests in property are generally based on exclusive control of the object, with pledgees possessing the pledged property to exclude interference from others, and mortgagees obtaining priority repayment rights through registration publicity. However, data has characteristics of replicability and shareability, making exclusive control difficult to achieve. After data is pledged, the pledgor may still possess usage rights, and even multiple creditors may claim security interests in the same data. This directly involves the basic principles of property law, namely object specificity and right excludability. According to Article 114 of the Civil Code, property right objects must be specified, but data has fluidity in physical form and variability in content, making specification challenging. Additionally, the excludability of security interests in property is to ensure the realization of creditors' claims, but the non-excludability of data may dilute security value or create rights conflicts, such as when data is pledged multiple times or licensed for use, making it difficult to determine creditors' priority ranking [4]. This legal conflict, on one hand, reflects the contradiction between data security and traditional theory, and on the other hand, demonstrates the necessity of reinterpreting security rules to adapt to new property forms in the digital age.

2.3. Limitations of existing mortgage and pledge interpretation approaches

Regarding the legal characterization of data security, the mortgage approach advocates treating data as intangible property and establishing mortgage rights through registration publicity. However, due to the dynamic changes in data content and unclear boundaries, it is difficult to achieve specification through description like real estate or equipment [5]. The characteristic of mortgage not transferring possession, in the data scenario, conversely becomes the pledgor's continuous use of data, resulting in unstable security value. The pledge approach simulates possession transfer by controlling data access rights or delivering encryption keys, but the replicability of data makes such control relative —pledgors or others can bypass restrictions to continue using data, thereby damaging the excludability of pledge rights. Additionally, existing interpretation approaches often ignore the multi-layered nature of data rights, such as pledging data resource holding rights, processing and use rights, and other sub-rights as a whole, aggravating unclear ownership and rights conflicts. From a normative analysis perspective, Article 440 of the Civil Code allows other property rights to be pledged, but whether data rights belong to such rights remains controversial, while mortgage rules rely more on enumerative provisions of tangible property or specific intangible property.

3. The foundation of data pledge eligibility from the perspective of rights bundle decomposition

3.1. The legal connotation of separation of data rights and sub-rights independence

The rights separation framework for data rights was developed to address the marketization and allocation of data production factors. Its core is to decompose data rights into three sub-rights: data resource holding rights, data processing and use rights, and data product operation rights. This decomposition does not create new rights but legally confirms different powers in the process of data value realization. Data resource holding rights refer to the legal control and custody of raw data, reflecting the legitimacy of data sources and initial control; data processing and use rights refer to the right to process, analyze, and apply data, reflecting creative labor in the data value-added process; data product operation rights refer to the transaction and benefits of data derivatives, reflecting the marketization dimension of data circulation [6]. From a civil law perspective, sub-

DOI: 10.54254/2753-7048/2025.30987

rights possess relative independence because they correspond to different stages of the data lifecycle and each has different power content and boundaries. Data processing and use rights can be exercised independently from holding rights, such as obtaining data processing rights through licensing agreements. This independence, to a certain extent, satisfies the requirements of the property right specificity principle, as each sub-right can achieve object specification by describing its specific content, scope, and application scenarios, rather than treating data as a vague whole [7]. From a legal connotation perspective, the separation draws on property rights separation theory, using power separation methods to resolve contradictions between data sharing and excludability, providing a more refined rights foundation for data pledge.

3.2. Analysis of the property rights attributes of data processing and use rights

Data processing and use rights are the core sub-rights in the rights separation, and their property rights attributes are key to demonstrating data pledge eligibility. This right is essentially a usufructuary control right, meaning the right holder's exclusive ability to analyze and process specific data and obtain benefits from it. From legal characteristics, data processing and use rights possess typical elements of property rights. First, they have control capacity—the right holder can directly control the data processing process and usage methods, such as extracting data value through algorithmic models. Second, they have profitability—the right holder can obtain economic benefits through data applications, such as improving operations or developing new products. Third, they have transferability—the right holder can license the right to others or use it for pledge financing. Therefore, data processing and use rights are closer to usufruct rights in the Civil Code. Although data is not tangible property, usufruct principles can be applied by analogy, treating it as a new type of property right. Specifically, Article 323 of the Civil Code stipulates that usufruct rights are "rights to lawfully possess, use, and benefit from real estate or movable property owned by others." While data processing and use rights do not involve physical possession of data, they serve a similar function through exclusive use and benefit from data value. The property rights attribute is also manifested in its pledgeability, as pledge requires the object to have assessable economic value and transferability, which data processing and use rights satisfy through specific application scenarios and benefit expectations [8]. Additionally, the property rights nature of this right is implicitly recognized in some judicial practices and academic theory—in data infringement cases, courts may protect data users' investment and benefit rights. Analyzing these attributes can clarify the object eligibility of data pledge and prevent the negation of its security value due to data's intangibility.

3.3. The role of independent sub-rights pledge in resolving excludability conflicts

Independent sub-rights pledge can resolve the legal contradiction between data non-excludability and security excludability. Data non-excludability means the same data can be used simultaneously by multiple parties, while security interests in property require exclusive control of the object to ensure priority repayment, creating a conflict that has long hindered the establishment of data pledge. By decomposing data rights into independent sub-rights and pledging sub-rights separately, excludability can be re-established to a certain extent. The pledge of data processing and use rights does not involve data as a whole but is limited to specific usage methods or application scopes, achieving object specification through defining power boundaries. This specification enables pledge right holders to exercise exclusive control over this sub-right, such as through registration publicity to exclude others' claims to the same usage method. From a legal theory perspective, this conforms

DOI: 10.54254/2753-7048/2025.30987

to the principle of property right object specificity, as the scope of sub-rights can be determined through descriptions of processing methods, data ranges, or application purposes, rather than relying on data's physical form [9]. Meanwhile, independent pledge eliminates problems caused by the non-excludability of data as a whole: multiple sub-rights can be pledged by different parties, but conflicts are reduced due to power separation [10]. Data holding rights and processing and use rights can be separately pledged to different creditors, each enjoying security interests within their power scope. This approach also conforms to the open provisions of Article 440 of the Civil Code regarding other property rights—as long as sub-rights possess property value and transferability, they fall within the scope of pledge [11]. The registration publicity system further strengthens excludability by disclosing sub-rights details, enabling third parties to know the rights burden situation and preventing duplicate pledges.

4. The doctrinal positioning and pledge eligibility of data processing and use rights

4.1. The basis for analogical application of civil code usufruct principles

Data processing and use rights can be doctrinally analyzed by analogical application of Civil Code usufruct principles, providing a legal theoretical basis for data pledge eligibility. Usufruct rights in traditional civil law are rights to use and benefit from others' property, with core characteristics of control, profitability, and term limitation. Article 323 of the Civil Code stipulates the basic scope of usufruct rights—possession, use, and benefit from real estate or movable property. Although data is not tangible property, data processing and use rights functionally possess property-like attributes. Data processing and use rights refer to the right holder's ability to process and analyze specific data and obtain economic benefits from it, with the right holder's exclusive control over data value conforming to the power structure of usufruct rights. The basis for analogical application is the similarity of legal purposes—usufruct rights promote optimal use of property, while data processing and use rights promote marketized circulation and value release of data production factors [12]. From a legal doctrinal perspective, analogical application requires similar conditions and consistent value evaluation. Data processing and use rights do not involve physical possession but achieve substantial control through controlling and using data content; their profitability is reflected in economic returns generated by data applications; term limitation can be defined through contracts or registration to limit the duration of rights. Additionally, Article 324 of the Civil Code regarding natural resource use rights also allows for expanded interpretation—natural resources as usufruct rights for intangible property provide a reference for new types of resources like data. Analogical application does not create new rights but accommodates new developments within existing legal frameworks, preventing excessive legal lag [13]. Analogy can, to a certain extent, resolve difficulties in data rights characterization, incorporating data processing and use rights into the usufruct rights category and laying the foundation for pledge eligibility. However, analogical application must consider differences caused by data characteristics—data replicability may weaken exclusive control, but this can be remedied through rights definition and registration publicity.

4.2. Analysis of legal requirements for data use rights as pledge objects

Data use rights as pledge objects must satisfy a series of legal requirements derived from general principles of security interests in property and specific provisions of the Civil Code. The primary requirement is object specificity—the pledge target must be clearly and specifically determinable. Data use rights can be specified by defining the scope, content, and application scenarios of data use

DOI: 10.54254/2753-7048/2025.30987

rights, such as limiting data sources, processing methods, and purposes, conforming to property right objects stipulated in Article 114 of the Civil Code. Specification can avoid ownership disputes caused by data ambiguity, making rights boundaries identifiable. Second, transferability is a pledge requirement—the pledge object should be legally transferable. Data use rights possess transferability; right holders can license others to use or dispose of their data use rights through pledge and other means, and the transfer of data use rights does not involve physical transfer of data itself, only power transfer. Article 440 of the Civil Code stipulates property rights pledge; data use rights are rights with economic value and fall within the transferable scope. Value capacity is another requirement—the pledge object should have assessable economic value. The value of data use rights is reflected in the benefits they can bring or costs they can save, such as improving operations or developing new products through data analysis [14]. Such value can be measured through market mechanisms or evaluation methods. Additionally, the legality requirement mandates that the pledge object has legal sources and compliant content, not infringing public interests or personal privacy, connecting with the Data Security Law and Personal Information Protection Law. Data use rights can serve as eligible pledge objects when satisfying specificity, transferability, value capacity, and legality requirements.

4.3. Inclusive interpretation of "other property rights" in Article 440 of the Civil Code

"Other property rights" in Article 440 of the Civil Code provide inclusive interpretation space for data use rights pledge, serving as the normative basis for data use rights pledge eligibility. This provision uses open-ended language to accommodate new types of property rights and prevent legal rigidity from enumerative listings. Data use rights are a new type of property right; incorporating them into the scope of "other property rights" requires purposive expansive interpretation. The basis for interpretation lies in legislative purpose: promoting the development of financing security and meeting the needs of economic practice [15]. Data use rights possess property rights attributes; as previously stated, data use rights have economic value, transferability, and specificity, similar to traditionally pledgeable rights like equity and intellectual property. From a systematic interpretation perspective, the Civil Code's property rights provisions regarding security interests have a functionalist orientation, emphasizing the economic substance of security over form. Data use rights pledge conforms to this orientation as it can effectively guarantee the realization of claims. Historical interpretation also provides basis—discussions during the legislative process regarding "other property rights" reflect inclusiveness. In the context of the digital economy, law needs to respond to new asset security demands. From a comparative law perspective, some jurisdictions recognize the pledge eligibility of data-related rights through similar expansive interpretation, providing reference for Chinese interpretation. However, interpretation should prevent excessive expansion from undermining legal stability. By explicitly defining data use rights as other property rights, pledge rules can be directly applied without separate legislation. Interpretation should consider rights substance rather than nomenclature, focusing on whether they possess core characteristics of pledge objects [16]. Judicial interpretations and practice will gradually establish inclusiveness, such as recognizing the effectiveness of data use rights pledge through case law.

DOI: 10.54254/2753-7048/2025.30987

5. Realization of sub-rights specification and registration publicity

5.1. The transformation of registration publicity function from ownership declaration to power definition

The registration publicity system's primary function in the traditional property rights system is to declare rights ownership—for example, real estate registration confirms owners to ensure transaction security [17]. However, in data pledge scenarios, registration publicity must transform from simple ownership declaration to power definition to adapt to the special attributes of data rights. The reason for this transformation is that data value realization depends on specific application scenarios and power details, not just general ownership claims. From a legal theory perspective, power definition conforms to the property right specificity principle—by registering descriptions of data usage methods, processing algorithms, application purposes, terms, and other elements, rights objects become sufficiently specific and identifiable, satisfying Article 114 of the Civil Code's requirements for property right objects. From a normative analysis perspective, this draws on intellectual property registration—patent licensing registration must disclose licensing scope, but data registration places more emphasis on describing dynamic powers. The change in registration function also reflects the needs of the data sharing economy, reducing rights conflicts and transaction uncertainty through precise power publicity.

5.2. Construction of registration content for data use rights pledge

The construction of registration content for data use rights pledge should center on power specification and risk control, with the core being rights element clarification through detailed description to achieve object clarity. Registration content should include declarations of data source legality, data scope definition, usage method description, application scenario limitations, benefit distribution mechanisms, and rights terms [18]. Data source legality ensures the pledge object complies with the Data Security Law and Personal Information Protection Law, noting data acquisition channels and anonymization processing to prevent legal defects [19]. Data scope definition must clearly identify the specific data sets involved. Usage method descriptions should detail data processing algorithms, analytical models, and output forms, such as labeling machine learning methods or statistical techniques, to reflect power uniqueness. Application scenario limitations define specific fields or purposes for data use, allowing use only for financial risk control or medical research, thereby restricting rights exercise scope. Benefit distribution mechanisms involve who owns economic benefits generated during the pledge period, such as agreeing that usage benefits first repay debts [20]. Rights terms specify pledge duration, preventing indefinite uncertainty. From a normative perspective, registration content must connect with Article 440 Civil Code pledge rules—registration content elements should sufficiently support the effectiveness of pledge contracts [21]. Additionally, standardization of registration content facilitates construction of a unified national registration platform, reducing difficulties in execution caused by regional differences.

5.3. Registration effectiveness system based on special needs of rights publicity

The special nature of data use rights pledge requires adopting a registration effectiveness system rather than a registration opposition system to address risks from data non-excludability and easy replicability. Registration effectiveness system means pledge rights are established only after

DOI: 10.54254/2753-7048/2025.30987

registration, enhancing rights certainty and priority ranking. The intangibility and shareability of data rights mean simple contractual agreements cannot oppose bona fide third parties—for example, unregistered pledges may be ignored by subsequent traders, creating rights conflicts. Registration effectiveness, through mandatory publicity mechanisms, makes pledge status publicly verifiable, preventing duplicate pledges or fraudulent behavior [22]. From a legal theory perspective, the registration effectiveness system conforms to property rights publicity and credibility principles—registration acts give pledge rights presumptive effectiveness, enabling third parties to make transaction decisions based on registration information [23]. For normative basis, Article 445 of the Civil Code's movable mortgage registration effectiveness rules can be applied by analogy, but adjustments must be made according to data characteristics. Data registration effectiveness should ensure timely updates of registration information to reflect data value changes, use blockchain evidence preservation to enhance immutability, and design simplified registration procedures to reduce compliance costs. Additionally, the registration effectiveness system increases transaction costs, but benefits outweigh costs—in data pledge scenarios, it can effectively resolve non-excludability conflicts and protect creditors' interests. In practice, registration effectiveness must combine with judicial protection—registered pledge rights enjoy priority repayment in bankruptcy procedures. However, the effectiveness system is not absolute and needs to consider exceptional circumstances such as emergency pledges, which can be remedied through temporary registration. Therefore, based on special needs of data rights publicity, the registration effectiveness system provides a stable legal foundation for pledge and promotes marketized circulation of data production factors.

6. Conclusion

The legitimacy dilemma of data asset pledge financing stems from contradictions between the special attributes of data rights and traditional security interest theory, with conflicts concentrated in the legal contradiction between data non-excludability and security excludability. Resolving this conflict requires breaking through the perspective of rights integrity and adopting a rights decomposition approach, viewing the bundle of data rights as a separable set of sub-rights: data resource holding rights, processing and use rights, and product operation rights. Among these, data processing and use rights, due to their direct control over data value and benefit rights, can be recognized as a type of property usufruct right through analogical application of Civil Code usufruct principles, satisfying the object requirements of security interests in property. Registration publicity mechanisms play a key role in achieving sub-rights specification by accurately describing rights content, scope, and application scenarios, making data use rights conform to the property right object specificity principle and subsequently incorporating them into "other property rights" stipulated in Article 440 of the Civil Code, demonstrating their pledge eligibility. This interpretive approach provides doctrinal basis for data pledge, reconciling contradictions between data sharing and security exclusivity through power separation and publicity strengthening, thereby promoting marketized circulation of data production factors. However, this framework may face practical tests—coordination between the detail level of registration content and trade secret protection, the dynamic characteristics of sub-rights value assessment, and other issues require improvement through subsequent judicial practice and rule refinement. The rights decomposition perspective provides a solid legal foundation for the development of data security systems and demonstrates the adaptability and innovation of property rights theory in the digital age.

DOI: 10.54254/2753-7048/2025.30987

References

[1] Gao, F. (2025). Data Assetization: The Legal Basis for Recognizing Data Assets on the Balance Sheet. Oriental La w, (05), 65–82.
[2] Luo, Y. (2025). Legal Realization of Financing Guarantees for Enterprise Data Assets. Politics and Law, (09), 160–176.
[3] Zhang, S. (2024). Legal Configuration for the Recognition of Data Assets on the Balance Sheet. China Legal Scienc e, (04), 229–249.
[4] Zhao, C. (2025). Data Trust: Theoretical Logic, Practical Obstacles, and Countermeasures. South China Finance, (0 6), 76–86.
[5] Zhang, S. (2025). The Systematic Construction of a Data Property Rights Registration System. Global Law Review, 47(04), 53–70.
[6] Kong, D., & Li, T. (2025). Data Assets as Capital Contribution: Theoretical Justification, Practical Dilemmas, and P athways to Breakthrough. South China Finance, (04), 63–75.
[7] Bao, X. (2025). On the Systematic Construction of the Data Property Rights Registration System. Jurist, (04), 50–60+191–192.
[8] Li, H. (2025). Examination and Improvement of the Eligibility of Data Assets for Capital Contribution. Oriental La w, (04), 107–123.
[9] Xuan, D., & Ni, K. (2025). Construction of a Sophisticated Regulatory Path for Capitalization Risks under the Reco gnition of Data Assets on the Balance Sheet. Journal of Financial Development Research, (06), 70–81.
[10] Yang, Y. (2025). Circulation Incentives and Institutional Responses for the Recognition of Data Assets on the Balan ce Sheet. China Business and Market, 39(08), 113–126.
[11] Zhao, T. (2025). The "Property-Economy" Separated Criminal Law Protection of Enterprise Data Assets. Chinese Criminal Science, (03), 89–105.
[12] Zhao, Z. (2025). Theoretical Justification and Rule Development for the Mortgage of Enterprise Data Rights. China Business and Market, 39(05), 114–126.
[13] Cheng, L. (2025). Legal Application of Enterprise Data Guarantee Financing. Jurist, (02), 67–80+193.
[14] Luo, Y. (2025). Data Property Rights Registration System: From Practical Exploration to Theoretical Construction —Based on the Perspective of Rights Confirmation and Transactions. Theory and Reform, (02), 74–91.
[15] Xu, H. (2025). On the Pledge of Enterprise Data Products: Underlying Logic and System Construction. Legal Foru m, 40(02), 55–67.
[16] Song, Q. (2025). Construction of a Data Property Rights Registration System with Chinese Characteristics. Rule of Law Research, (02), 3–17.
[17] Zhao, Z. (2025). Data Asset Financialization: Chinese Practice and Prospects. Finance and Accounting Monthly, 46 (04), 33–38.
[18] Zhang, S., Zhao, S., & Yan, R. (2024). Research on the Realization of Enterprise Data Asset Value and Financial Su pport Models. Southwest Finance, (10), 42–52.
[19] Zhang, Z. (2024). The Logical Shift, Core Framework, and Optimization Strategies of the Data Asset Registration S ystem. Governance Studies, 40(06), 123–139+160.
[20] He, Y., Chen, L., & Du, Y. (2024). Can Data Assetization Alleviate the Financing Constraints of Specialized, Sophis ticated, Distinctive, and Novel SMEs? China Industrial Economics, (08), 154–173.
[21] Peng, C., & Gong, S. (2024). Theoretical Clarification and Normative Construction of Public Data Asset Pledges. L aw Science Magazine, 45(05), 36–52+2.
[22] Lu, X., & Li, J. (2025). The Impact of Data Assetization on Corporate Debt Financing Costs. Journal of Industrial T echnological Economics, 44(09), 77–86.
[23] Tan, Z. (2024). On the Institutional Construction of Data Property Rights Registration. Contemporary Law Review, 38(04), 86–97.