Research on the Configuration of Rights Intensity in Data Rights Confirmation

Zhang Man¹ Liu Zhengming²

2026-07-06

ChinaRxiv

Abstract

[Purpose/Significance] Against the backdrop of data factorization, full-chain utilization, and cross-scenario circulation, this paper constructs a differentiated allocation framework centered on the intensity of rights, aiming to provide theoretical reference and institutional directions for resolving the dual dilemma of fragmented rights and centralized control. [Method/Process] Data classification-based rights determination is defined as an institutional generation mechanism. Three criteria from law and economics—incentive mechanisms, externalities and risk diffusion, and institutional friction—are introduced to establish corresponding relationships with rights structures, behavioral rules, and liability mechanisms. On this basis, institutional analysis is conducted with the differentiated allocation of rights intensity as the main line. [Results/Conclusion] Data rights determination should combine different data types and differentially allocate rights intensity and governance measures. Personal data should adopt limited-strength allocation and enhanced liability density; enterprise data should be relatively strengthened while subject to constraints of competitive order; public data should adhere to minimal exclusivity and rule-based openness.

Full Text

Research on the Configuration of Rights Intensity in Data Rights Confirmation

Zhang Man1　Liu Zhengming2

(1. School of Economics and Management, Shanghai University of Political Science and Law, Shanghai 201701;
2. Qingpu District Human Resources and Social Security Bureau of Shanghai Municipality, Shanghai 201799)

Abstract: [**Purpose/Significance**] Against the backdrop of the factorization of data, full-chain utilization, and cross-scenario circulation, this study constructs a differentiated configuration framework centered on rights intensity, aiming to provide theoretical reference and directions for institutional design to address the dual dilemma of rights fragmentation and centralized control. [**Method/Process**] Data classification and rights confirmation are defined as an institutional generation mechanism. Three criteria from law and economics —incentive mechanisms, externalities and risk diffusion, and institutional friction—are introduced, so that they correspond respectively to rights structures, behavioral rules, and liability mechanisms. On this basis, institutional analysis is carried out with the differentiated configuration of rights intensity as the main thread. [**Results/Conclusions**] Data rights confirmation must be combined with different types of data, with rights intensity and governance tools configured differentially. Personal data should adopt constrained-intensity configuration and increased liability density; enterprise data should be relatively

strengthened while being subject to constraints of competitive order; public data should adhere to minimal exclusivity and rule-based openness.

Keywords: data rights confirmation; rights intensity; law and economics; externalities; institutional friction

Classification numbers: G203 D912.1

DOI: 10.31193/SSAP.J.ISSN.2096-6695.2026.02.04

0 Introduction

The factorization of data promotes the movement of data from organized resources into the factor market, and the institutional pressure arising from this is concentrated in the issue of the sustainability of circulation governance. As data becomes cyclically embedded in the chain of collection, processing, sharing, and reuse, the distribution structure of data ownership gradually shifts from "one type of data corresponding to one product" to "one item of data involving multiple forms of processing," and the forms of legally protected interests likewise present a compound and overlapping pattern involving multiple subjects and multiple attributes [1]. Against this background, the practical difficulties of data circulation do not necessarily stem from the absence of rights; rather, they arise more often from an imbalance in the rights structure. On the one hand, fragmentation of rights can easily accumulate negotiation and enforcement costs within authorization chains that require permissions step by step, person by person, and purpose by purpose, thereby making effective data utilization difficult. On the other hand, although centralized control reduces authorization nodes, it may solidify into a barrier to market entry and compress the space for subsequent innovation and competition through selective licensing, differentiated conditions, and blocked interfaces [2]. Therefore, the institutional meaning of rights confirmation should be understood as forming an operable balance among the boundaries of use, chains of responsibility, and intensity of control, so that the system can operate stably. The realization of such a balance depends on forming differentiated rights intensity, tolerance boundaries, and responsibility structures according to the interest structures, risk distributions, and circulation needs of different data types [3].

[**Author biographies**] Zhang Man, male, master' s student, research focus: law-and-economics analysis, Email: 598639769@qq.com; Liu Zhengming, female, research focus: procedural law, Email: 295820199@qq.com.

1. The Problem-Generating Logic and Classification Starting Points of Data Rights Confirmation Disputes

1.1 Object Demarcation and the Dilemma of Unified Rights Confirmation

In discussing data rights confirmation, it is first necessary to clarify the boundary of the concept of "data" so that issues such as incentive mechanisms, externalities and risk diffusion, and institutional friction can be discussed under the same premise. In current academic debates, objections to data rights confirmation often take the attributes of information as their starting point, directly applying to data such features as the public-good characteristics of information, the difficulty of clearly defining its boundaries, and the difficulty of separating content from source. They thereby reach the conclusion that data lacks independence and exclusivity and thus cannot be subject to rights confirmation. If one simply responds to the above views by invoking the exclusionary logic of traditional ownership, the same obstacle arises: data can be copied, used by multiple parties, and continuously circulate through different processing stages, making it difficult for rights boundaries to stabilize in the same way as those of tangible objects. It can therefore be seen that the two views— "data cannot be subject to rights confirmation" and "data should be owned by someone" —in fact both stem from the failure to clarify the object premise, exposing the structural predicament inherent in the very discussion of rights confirmation. On this basis, it is necessary to distinguish information from data. Data is closer to symbolic records that can be processed automatically; under specific temporal and processing conditions, it has a relatively clear basis for identification and is therefore more suitable as an object of institutional allocation. Information, by contrast, is closer to semantic content and forms of expression, and its boundaries are more easily affected by context and carrier. Although information and data can be transformed into each other along technical pathways, this transformability does not mean that the two may be treated interchangeably in institutional design. Only by distinguishing them at the object level can one avoid directly taking judgments about the attributes of information as the institutional premise for data rights confirmation [4].

1.2 The Embedding of Multiple Interests and the Emergence of Issues Concerning the Intensity of Rights

Throughout the entire chain of collection, processing, circulation, and reuse, the same set of data always carries the different interest claims of multiple subjects. As application scenarios change and technical combinations are adjusted, the weight of these interests and the boundaries of rights also continuously shift. In other words, the interest structure attached to data is dynamic and scenario-based. This makes it difficult for rights-confirmation discussions to remain at the abstract level of naming rights; the focus of argumentation must inevitably sink into questions concerning the allocation of rights intensity, boundaries for accommodating others, and liability structures. At the same time, the design

of data institutions should also consider the embedding of rules for "conduct-based regulation," so as to respond to the differentiated constraints imposed by different types of data in circulation, utilization, and risk control [5].

More specifically, the release of data value depends heavily on scaled processing and cross-scenario reuse. This leads to asymmetry between the ability to control data and the possible scope of influence generated by data. For example, one subject may legally control data, but the risks triggered after data is aggregated, inferred from, and re-identified may extend far beyond the boundary between the original parties to the transaction, affecting unspecified third parties and even the public interest. At the same time, data that was originally dispersed and of relatively low sensitivity may, after aggregation, generate new and highly sensitive information, pushing conflicts from the level of individual interests to the level of competitive order and public governance. This effect, whereby quantitative change gives rise to qualitative change, further reinforces the necessity of using "behavioral boundaries" and "responsibility chains" to absorb institutional conflicts.

1.3 Criteria and References from Extraterritorial Institutional Pathways

Although extraterritorial data governance has formed different institutional pathways, structurally these can largely be summarized as different balances among incentive mechanisms, externalities and risk diffusion, and institutional friction. The institutional practices of the European Union, the United States, and Singapore provide reference models for observing differences in the intensity of rights, the density of rules, and the allocation of responsibility in the classification-based confirmation of data rights.

The EU pathway can broadly be summarized as strong-rule governance under high-risk constraints, supplemented by mechanisms for sharing and availability. In the field of personal data, the EU' s *General Data Protection Regulation* (GDPR) imposes strengthened constraints on the spillover of personality-related risks and on harms that are difficult to reverse, through rights bundles, compliance obligations, and accountability mechanisms. This reflects an institutional orientation that uses externality criteria to limit exclusion intensity and reduces regulatory and relief costs through procedural obligations. In the field of non-personal data and the circulation of public-sector data,

The EU has also, through arrangements concerning reuse, data intermediaries, availability, and interoperability in the *Data Governance Act* and the *Data Act*, reduced friction in multi-actor collaboration by means of regulatory tools and organized mechanisms, without directly increasing the strength of exclusionary rights [6–7].

The U.S. approach displays the characteristics of fragmented legislation centered on the boundaries of market conduct. State-level practices represented by the *California Consumer Privacy Act* (CCPA) and the *California Privacy Rights*

Act (CPRA) have not moved comprehensively toward high-density regulation; rather, they construct institutional boundaries around consumer control, opt-out mechanisms, and constraints on corporate conduct. Through institutional arrangements such as "refusal to sell or share," "correction," and "deletion," they compress the space for enterprises' unilateral control over personal information, and reduce the cost of case-by-case negotiation through relatively standardized opt-out and response procedures.

The Singaporean approach is closer to a balanced compliance framework guided by risk governance. After the amendment of Singapore' s *Personal Data Protection Act* (PDPA), institutional tools such as data-breach notification, organizational obligations, and accountability mechanisms have strengthened the controllability and traceability of risk incidents. Compared with simply increasing the strength of exclusion, this path places greater emphasis on achieving risk convergence through continuous compliance, process control, and responsibility mechanisms, while maintaining stable governance effects with relatively low institutional friction [8].

2 Three-Dimensional Criteria of Law and Economics

2.1 Incentive Mechanism

The incentive-mechanism criterion examines whether different institutional arrangements can generate stable input. If inputs are difficult to identify, returns cannot be recovered, and exclusionary boundaries are difficult to enforce, rights confirmation will be unable to create substantive incentives; instead, it may easily cause incentive distortions and push up governance costs. Specifically, incentive logic needs to satisfy three basic conditions:

First, inputs should be identifiable. The formation and value release of data are usually embedded in technical systems, business processes, and multi-actor collaboration. If contributions cannot be reasonably decomposed, the rights configured by the institution will be difficult to match with the actors that truly undertake key inputs and risks [9]. Once the object of the incentive deviates, investors will be unable to form stable expectations of returns, and the incentive function of rights confirmation will thereby lose its foundation.

Second, returns should be recoverable. This does not mean that exclusionary control should be continuously strengthened [10]. The value of data inherently depends on repeated use and continuous processing. If "return recovery"is simply understood as continuously strengthening exclusionary rights, it will instead raise negotiation, compliance, and transaction costs in multi-actor collaboration and multi-scenario use, leading to a rapid increase in institutional costs [11]. A more feasible approach is to maintain a balance between return recovery and appropriate openness through use restrictions, responsibility mechanisms, and transaction rules, implementing the protection of returns at enforceable boundaries of use rather than continuously expanding exclusionary control.

Third, exclusionary boundaries should be implementable. If rights boundaries are difficult to identify and enforce in disputes, rights confirmation will continually trigger boundary disputes, and the resulting rise in institutional costs will in turn weaken the incentive effect. Especially under conditions of diverse data uses and incomplete information, it is difficult to finely manage specific use behavior by relying solely on exclusionary control [12]. Therefore, the institutional focus should be moved forward to the level of rule design: by directly constraining conduct and structurally allocating responsibilities, the focus of disputes can be narrowed to verifiable questions of "which acts are permitted and which acts entail responsibility."

2.2 Externalities and Risk Diffusion

The externalities-and-risk-diffusion criterion examines whether different institutional arrangements can effectively control the spillover of risks and their consequences. The impact of data-processing activities often spills beyond the scope of contractual counterparties, affecting unspecified third parties and even the public interest; moreover, such spillover effects are difficult to fully absorb within existing frameworks of rights and obligations. As data-processing chains extend, externalities may also exhibit delayed impacts and risk

an accumulative form of expansion and, as time passes and the number of participating actors increases, continuously diffuses outward. This makes traditional risk-control models centered on one-time authorization or single-point control unable to effectively contain risks.

Structurally, such externalities are mainly manifested at two levels. First, they intrude upon the interests of actors other than the counterparty. In the course of data use, data may affect third parties without being fully identified and disclosed, and may, through algorithmic profiling, social scoring, and similar methods, exert long-term and implicit interventions in their social evaluation, development opportunities, and even behavioral patterns [13]. Second, they distort market structures and public order. When data-control capacity is deeply coupled with competitive advantage, the entities that possess data may, through selective supply, differentiated pricing, raising rivals'access thresholds, and other means, transform private control into barriers to market entry, thereby entrenching advantages and exacerbating structural inequality [14].

This diffusion mechanism is especially evident in the field of personal data. Once data enter large-scale processing and correlational analysis, they often continue to ferment through re-identification and profiling inferences, producing long-term effects on personal dignity, privacy, and social evaluation. Reliance solely on exclusive control at the initial stage is not only insufficient to cover subsequent complex use scenarios, but may instead increase governance costs because of the fragmentation of rights [15]. Moreover, some externality consequences are irreversible or difficult to restore, such as the actual impacts caused by algorithmic discrimination or social scoring, which are difficult to fully remedy after the

fact through "restoration to the original state" or "injunctions." Therefore, the institutional focus must be appropriately moved forward, shifting more toward duties of care, compensation mechanisms, and allocation of responsibility, so as to compress the space in which risks arise through enforceable rules of conduct.

2.3 Institutional Friction

The criterion of institutional friction examines whether different institutional arrangements can reduce circulation costs and maintain a stable order of transactions. Once data elements enter tradable stages, friction is not confined to obstruction in a single link, but gradually accumulates along the entire transaction chain. For example, before a transaction, information must be identified and risks verified; during the transaction, authorization must be negotiated and terms coordinated; after the transaction, boundaries must be maintained and disputes handled. In addition, audit, accountability, and other supervisory work run through the entire process. The more complex the collaborative network formed by data use, the more evident the shaping effect of the initial rights structure on the forms of friction.

If rights are divided too finely, the number of authorization nodes and verification obligations will be magnified. Each additional node that requires consent raises negotiation costs accordingly. Once a delay occurs at an irreplaceable node, the entire collaborative chain may be interrupted, and problems of resource allocation can very easily trigger negotiation failure. At the same time, the more dispersed the actors are, the more complicated it becomes to identify uses that exceed boundaries, allocate responsibility, and preserve evidence; the pressure of enforcement and supervision also rises significantly at a structural level [16]. Conversely, if rights are excessively concentrated, although authorization nodes may appear to decrease, the controller may transform its control advantage into barriers to market entry by refusing provision, granting selective licenses, imposing differentiated conditions, or blocking interfaces. At this point, institutional friction is no longer mainly manifested as cumbersome authorization, but more as reduced transaction opportunities, restricted substitute pathways, and the contraction of data-circulation space into a scope of permission controllable by a small number of actors. Meanwhile, data transactions cannot be completed through a single authorization or a single delivery. After a transaction is concluded, continuing issues remain, such as boundary maintenance, use verification, and responsibility tracing. If the authorized content is unclear and the scope of use is ambiguous, then once a dispute arises, the focus can easily return to ex post proof and determination of responsibility, causing enforcement costs to rise. The same is true of supervision: the more blurred the behavioral boundaries, the more repeated inspections and supplementary explanations are needed to maintain order, and the burden of handling disputes after the fact will increase accordingly.

3 Rights-Strength Configuration Guided by Three-Dimensional Criteria

3.1 Classification Standards and Rights-Strength Configuration

Classification is first of all an ex ante configuration mechanism, whose function is to discuss specific rights strength, circulation conditions, and responsibility structures.

Before this, basic institutional presumptions should first be made for different types of data. Once classification criteria enter institutional operation, they will continue to affect subsequent institutional costs and market behavior. If classification remains merely a formal enumeration of types, institutional design can easily fall into the binary opposition of "either full protection or no protection at all," making it difficult to provide switchable institutional interfaces for different risk scenarios and utilization objectives.

Whether a classification is reasonable must ultimately be tested by the effects of institutional operation. Any classification criterion detached from the core objective of configuring the intensity of rights is liable to become a merely formal division; it will be difficult either to reduce the operating costs of the institution or to provide substantive guidance for data circulation and innovation.

On this basis, the intensity of rights should be understood as an operable configuration variable, which may specifically take the form of a flexible combination of such elements as exclusion boundaries, scope of access, duration, possibilities for re-sharing, and methods for handling derivative results [17]. Accordingly, the configuration of rights intensity is constrained by risks at both ends: if exclusivity is too strong, it can easily induce fragmentation of rights and lead to failure of collaboration; if boundaries are too weak, they will be insufficient to secure recovery of investment and allocation of responsibility. A more feasible path is to establish, by category, the minimum necessary foothold of rights and powers, and, on that premise, to procedurally embed tolerance boundaries, fair use, attribution of responsibility, and supervisory obligations into the rights structure, so that the intensity of rights remains adjustable and can operate stably.

3.2 Coupled Configuration of Rights Structures, Behavioral Rules, and Responsibility Mechanisms

To implement the above classification logic at the normative level, it is necessary, on the basis of the nomenclature of rights, to further form institutional arrangements capable of covering continuous use, changes of purpose, and responsibility tracing. While retaining a minimum foundation of rights, the institutional differences among different types of data should be implemented primarily through rules of use, behavioral constraints, and allocation of responsibilities, thereby avoiding placing all complex governance tasks upon a single form of right [18-19].

Among these, the basic rights structure does not cover all powers, but rather

provides tradable modules of powers. Through the modular decomposition of powers such as control, use, 收益, and licensing/disposition, identifiable and combinable boundaries and interfaces are provided for subsequent circulation [20]. The regulatory system of behavioral constraints performs the function of continuously supplying boundaries for purpose migration and derivative use, so that the parties to a transaction need not cover all future uses through exhaustive negotiation, and so that the focus of supervision can be narrowed to verifiable boundary-crossing conduct [1]. The responsibility-allocation mechanism, in turn, uses procedural obligations, triggering conditions, and allocation of evidentiary burdens to align risk-bearing with control capacity and scope of influence, thereby both preventing supervision costs from being structurally shifted and avoiding over-dense regulation.

Under this structure, the three-dimensional criteria correspond to the coupled configuration: the incentive-mechanism criterion is used to examine the necessity of the basic rights structure and the boundary settings of rights-and-powers modules; the criterion of externalities and risk diffusion operates on the upper limit of exclusivity intensity within the regulatory system of behavioral constraints, and limits risk spillover through boundaries of use; the institutional-friction criterion is used to identify high-friction points in negotiation, implementation, and supervision, and on that basis to introduce standardized interfaces and verifiable processes, so that rights boundaries can be replicated and subjected to external examination.

4 Institutional Construction Orientation Based on Differentiated Configuration of Rights Intensity

4.1 Limited-Intensity Configuration of Personal Data and Enhancement of Responsibility Density

Personal data should be governed primarily through limited-intensity configuration, supplemented by higher-density rules and responsibility mechanisms to undertake governance tasks. The reason is that, within the institutional structure, personal data simultaneously involves human dignity, economic utilization, and public risk; it has the strongest composite character, and its exposure to externalities is also the most extensive [21].

In terms of risk distribution, once personal data enters large-scale processing and correlation analysis, its effects will exceed the initial transactional relationship and will continuously diffuse in subsequent use, thereby affecting privacy protection, social evaluation, and even development opportunities. Such effects often do not appear on the spot, but instead accumulate gradually in subsequent processing and continuous use. Therefore, the traditional one-off notice-and-consent mechanism can hardly cover—

cover the continuously extending chains of use[^22]. In practice, anonymization and de-identification do not necessarily eliminate personality-related risks; ex-

ternalities may still be re-aggregated in subsequent stages through inference and re-identification, and transformed into perceptible harm[^23]. For example, the Court of Justice of the European Union has interpreted the applicable boundaries and information-disclosure obligations for automated processing such as credit scoring, emphasizing that automated profiling may have substantive effects on individuals' opportunity structures, thereby triggering stronger procedural safeguards and accountability requirements[^24]. Italy' s sanction against the U.S. facial-recognition technology company Clearview AI also shows that, even where data are publicly accessible, the relevant processing activities may still be brought under high-intensity compliance constraints because of risks of re-identification and inference[^25]. The Personal Data Protection Commission of Singapore (PDPC) found that Marina Bay Sands failed to implement access controls and security configurations during the migration from old to new system software, resulting in the unlawful acquisition and leakage of large-scale personal data. The enterprise had not established institutional security arrangements commensurate with the level of risk, thereby violating its data-protection obligations, and was penalized accordingly[^26]. These cases show that the focus of personal-data governance should not be placed on ownership-style exclusive control, but should instead shift toward continuous constraints on boundaries of use, processing procedures, and chains of responsibility.

The so-called "limited-strength configuration" of personal data may be defined as follows: retaining the minimum necessary rights fulcrum, while imposing strict constraints on exclusivity and transferability, and taking rules of use and responsibility structures as the institutional axis. First, individuals should still retain the basic rights fulcrum needed to maintain their status as subjects and to initiate remedial procedures. Second, the intensity of exclusivity should correspond to the degree of risk associated with processing activities and should not be strengthened in an undifferentiated, integrated manner. Third, institutional boundaries should be fixed primarily within acts of use and procedural obligations; through purpose limitation, minimum necessity, conditions for onward sharing, and accountability chains, the focus of protection should shift from "who owns the data" to "how the data are used." Fourth, it is also necessary to prevent processors from forming an unchallengeable position of absolute control, and to reserve institutional interfaces for subsequent constraints on use and allocation of responsibility[^27]. From the perspective of institutional friction, personal data are highly dispersed, and multi-party participation and repeated use are the norm. If every instance of processing is required to depend on high-intensity exclusive authorization, compliance costs and negotiation costs will rise significantly, and in scenarios of large-scale use will create a de facto entry threshold, compressing the space for reasonable circulation under the premise of legality and compliance.

Therefore, the limited-strength configuration of personal data should take the legal bases, purpose limitation, and minimum necessity established by the *Personal Information Protection Law of the People' s Republic of China* as its basic boundaries, and should be connected with the classification and grading as well

as risk-assessment requirements of the *Data Security Law of the People' s Republic of China*. In this way, "limited strength" should be implemented as ex ante constraints on the expansion of uses, processing chains, and high-risk activities. Specifically, it can be summarized in three respects: first, limiting the expansion of the scope of processing through use control and change assessment; second, establishing processing chains that are auditable and accountable; and third, setting higher thresholds for automated decision-making, the processing of sensitive personal information, and cross-border flows.

4.2 Relative Strengthening of Enterprise Data and Constraints of Competitive Order

The institutional design of enterprise data should maintain a balance between incentives for investment and competitive order. If ownership-style exclusivity is applied mechanically, it is easy to solidify enterprises' control over data into barriers to market entry; if only factual control is recognized without normative guidance, a platform's technological advantages may be improperly transformed into a dominant position. The appropriate path is, while recognizing enterprises' relatively stronger demand for incentives in relation to data, to set boundaries for concentrated control through anti-abuse rules and availability rules, thereby forming a coexistence of "relative strengthening + structural constraints."

Enterprise data are more readily explained by incentive logic, mainly because the formation of their value depends heavily on continuous investment and organized governance. Their investment chains are relatively clear, and business risks are more predictable; once the boundaries become unstable, however, problems of free-riding and outflow of returns are more likely to arise, thereby weakening expectations for subsequent supply and cooperation[^28]. In view of this, appropriately increasing the stability of enterprises' control over data helps to anchor expectations of investment recovery in identifiable and verifiable fulcrums of legal capacity, providing a comparatively stable institutional foundation for data-driven innovation.

At the same time, this strengthening remains highly sensitive to collaborative scenarios and market structures. Enterprise data are often situated at the intersection of competition and cooperation. If the boundaries of exclusivity are not constrained, control capacity may, through selective supply, differentiated conditions, or interface foreclosure, be transformed into de facto

de facto entry barriers, thereby solidifying the competitive landscape and raising the costs for new entrants [29–30]. In practice, platform data scraping and interface blocking have already generated typical conflicts. Taking the U.S. case *hiQ Labs v. LinkedIn* as an example, with respect to the dispute between the scraping of publicly accessible data and a platform' s blocking and control measures, judicial practice has shown that the strengthening of rights in enterprise data cannot be directly equated with exclusive control; rather, it must remain subject to the continuing constraints of the competitive order and anti-abuse

rules [31]. Therefore, the relative strengthening of enterprise data should be embedded within the framework of the competitive order. The exercise of such rights should be constrained through antitrust law, anti-unfair-competition law, and sectoral regulation, so that the strengthening of rights is confined to the extent necessary to incentivize investment [32].

At the same time, the configuration of the intensity of enterprise-data rights should also be implemented through executable transaction structures, so as to avoid creating high-friction chains in contract negotiation, evidentiary proof of performance, and continuous supervision. In practice, enterprise data are often shared and used through contracts, platform rules, or industry cooperation mechanisms. If the rights structure is overly rigid, it will increase negotiation costs and suppress cross-entity collaboration and data integration [33]. On this premise, while relative strengthening should be recognized at the classification level, room should also be reserved for contractual arrangements and regulatory intervention. Through mechanisms such as standardized interfaces, traceable records of calls, and accountability tracing, the stability of control can be combined with the flexibility of circulation.

The coordinated implementation of "relative strengthening + structural constraints" for enterprise data should be aligned with the rules of the *Anti-Unfair Competition Law of the People' s Republic of China* on improper acquisition, use, and disruption of competitive order, and should also be linked to the classification and grading, important-data management, and security obligations under the *Data Security Law of the People' s Republic of China*. This can be further refined into three arrangements. First, on the premise that the input can be identified, the basis of rights should be defined and a verifiable boundary of control should be formed. Second, in contexts where platform control is strong and data resources are highly concentrated, requirements of reasonable openness, nondiscriminatory supply, and anti-abuse constraints should be introduced to prevent interface blocking and data barriers. Third, mechanisms such as traceable records of calls, hierarchical licensing, and security assessment should be used to reduce the costs of implementation, evidence collection, and supervision.

4.3 Minimum Exclusion and Rule-Based Opening of Public Data

The legitimacy of public data lies in the realization of public purposes and in scalable openness and usability. Accordingly, its institutional design need not rely on an ownership-style logic of exclusion. Rather, on the premise of minimum exclusion, it should take rule-based openness, conditional reuse, and accountability supervision as its principal tools, thereby safeguarding sustained use oriented toward the public interest [34].

Public data are usually generated by public institutions in the course of lawfully performing their duties and providing public services, and their generation does not take the input–return of a specific entity as the primary consideration. At

the same time, the value of public data often increases as the scale of use expands and the modes of utilization diversify. Exclusive allocation does not generate substantive incentives; instead, it may constrict the space for sharing and raise institutional friction costs. This is especially true of public-administration data: the authority and responsibilities for processing such data derive directly from legal norms, and therefore they are not suitable to be possessed by individual entities through exclusionary means or freely transferred.

The intensity of rights in public data should adopt the basic orientation of "minimum exclusion," placing the institutional focus on executable arrangements for rules on openness, boundaries of use, and risk control. The opening of public data generally has positive externalities in reducing transaction costs, increasing transparency, and supporting innovation, and the realization of its value depends on broad access and scaled utilization. Once overly strong exclusionary control is imposed, public resources may be occupied by a small number of entities and converted into new market-entry barriers. At the same time, rule-based openness should proceed on the premise of security review. Where matters such as national security, important data, personal information, and privacy are involved, controllable openness must be maintained through ex ante mechanisms such as graded access, restrictions on use, and risk assessment.

In institutionalized utilization scenarios, authorized operation may serve as an organizational form for realizing the value of public data, but its legitimacy depends on stronger procedural constraints and supervisory chains, so as to prevent "practical exclusion" from hollowing out the configuration of minimum exclusion. In other words, even if an operating institution obtains an operational position on the basis of authorization, it must not re-privatize public data through discriminatory conditions, interface blocking, or exclusion of redevelopment. Conversely, authorized operation should take open competition, nondiscriminatory access, and the prohibition of exclusive authorization as its basic requirements, and should do so through auditable

through process management, complaint and appeal procedures, and external oversight mechanisms, thereby maintaining a balance among controllability, usability, and beneficial use [35].

Accordingly, the "minimum exclusivity" of public data should be further implemented as a combined structure of openness rules, use boundaries, risk assessment, and accountability oversight. Its institutional expression may be summarized in three respects: first, defining the scope of openness through public-data catalogs, open lists, and use restrictions; second, maintaining open competition, non-discriminatory access, and prohibitions on exclusive authorization in authorized operations, so as to prevent de facto monopolies; and third, ensuring—through security assessment, desensitization processing, tiered access, and external supervision mechanisms—that the open use of public data remains constrained by national security, protection of personal rights and interests, and public-interest objectives.

5 Conclusion

This paper reconstructs data-rights determination as a question of allocating rights intensity and governance tools. Taking incentive mechanisms, externalities and risk diffusion, and institutional friction as three constraining criteria, it seeks an enforceable institutional equilibrium through differentiated arrangements of rights intensity and the embedding of behavioral rules and liability mechanisms. In concrete allocation, personal data should emphasize limited-intensity arrangements and greater density of responsibility in order to respond to high-risk externalities; enterprise data should adopt relatively strengthened rights supplemented by constraints of competitive order, so as to accommodate both investment incentives and market openness; and public data should take minimum exclusivity and rule-based openness as its basic orientation, thereby safeguarding scaled utilization under a public-interest orientation.

This study still has certain limitations. On the one hand, its analysis is mainly based on doctrinal and comparative perspectives, and it still lacks systematic empirical testing of the operational effects of different institutional pathways. On the other hand, the boundaries for applying the three-dimensional criteria in concrete scenarios remain to be further tested and refined through additional judicial practice and regulatory cases. Future research may combine data-circulation models and enforcement practice in specific industries to conduct more detailed empirical analysis of the actual effects of rights-intensity allocation, thereby further enhancing the operability and explanatory power of institutional design.

【References】

[1] Guo Ziyi. Beyond data property rights: a legal response to a data-rights attribution system for multiple interest claims [J]. Journal of Dalian University of Technology (Social Sciences), 2025, 46(5): 85–92.

[2] Gordon W J. Fair use as market failure: a structural and economic analysis of the Betamax case and its predecessors [J]. Columbia Law Review, 1982, 82(8): 1600–1657.

[3] Ma Feicheng, Xiong Siyue, Sun Yujiao, et al. The impact of data classification and grading rights determination on realizing the value of data elements [J]. Journal of Information Resources Management, 2024, 14(1): 4–12.

[4] Xiang Dingyi. On data-rights determination based on the binary distinction between information and data [J]. Credit Reference, 2025, 43(11): 36–46.

[5] Li Sanxi, Zhang Mingsheng, Wang Taiming. Rights determination and regulation of data elements: model innovation and impact mechanisms [J]. Journal of Beijing Jiaotong University (Social Sciences Edition), 2025, 24(3): 36–43.

[6] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Reg-

ulation (EU) 2018/1724 (Data Governance Act) [EB/OL]. [2026-02-14]. http://data.europa.eu/eli/reg/2022/868/oj.

[7] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [EB/OL]. [2026-02-14]. http://data.europa.eu/eli/reg/2023/2854/oj.

[8] Singapore Statutes Online. Personal Data Protection (Amendment) Act 2020 (No. 40 of 2020) [EB/OL]. [2026-02-14]. https://sso.agc.gov.sg/Acts-Supp/40-2020/.

[9] Sun Jimin. Data-rights determination from the perspective of incentive theory [J]. Legal Forum, 2025, 40(6): 150–161.

[10] Solow-Niederman A. Information privacy and the inference economy [J]. Northwestern University Law Review, 2022, 117: 357–424.

[11] Zhu Qiantao. The practical dilemmas, systematic construction, and promotion path for the circulation of data elements under the separation of three rights [J]. China Business and Market, 2025, 39(12): 43–57.

[12] Merrill T W, Smith H E. The property/contract interface [J]. Columbia Law Review, 2001, 101: 773–852.

[13] Hu Chaoyang. Legal regulation of personal information processing in the context of big data: An analytical perspective based on the dual externalities of personal information processing [J]. Journal of Chongqing University (Social Science Edition), 2020, 26(1): 131–145.

[14] Sun Ying. Research on mechanisms for defining rights in and authorizing enterprise data [J]. Comparative Law Review, 2023(3): 56–73.

[15] Xu Yongguo. Collective governance of personal data: Concepts, models, and mechanisms [J]. Study and Exploration, 2025(11): 42–54.

[16] Zhao Xu. The issue of fair use of generative artificial intelligence in machine learning [J]. Journal of Jinan University (Philosophy and Social Sciences Edition), 2024, 46(3): 79–95.

[17] Xiang Chao, Fang Chaoyi. Research progress on data rights confirmation under the structural separation of property rights [J]. Journal of Chongqing University of Technology (Social Science), 2025, 39(7): 133–146.

[18] Guo Xuejiao, Nie Yanfang. Data rights confirmation as a means of realizing data governance [J/OL]. Library, 1–7 [2026-05-03]. https://link.cnki.net/urlid/43.1031.G2.20251112.1025.008.

[19] Jiang Huiling, Li Jiashuo. The jurisprudential dilemmas and solutions for data rights confirmation in China [J]. Academic Exchange, 2025(4): 60–73.

[20] Zhang Xinbao. On data property rights as a new type of property right [J]. Social Sciences in China, 2023(4): 144–163, 207.

[21] Wang Yuchen, Ouyang Rihui. Paradigm transformation and governance strategies of data governance in the digital economy era: From the perspective of the awakening of personal data consciousness [J]. Macroeconomics, 2025(8): 11-26.

[22] Xu Wei. On the algorithmic identification characteristics of personal information and their normative significance [J]. Law Forum, 2025, 40(6): 79-90.

[23] Shen Weixing. Debate on data rights confirmation [J]. Comparative Law Review, 2023(3): 1-13.

[24] Court of Justice of the European Union. EUR-Lex - 62022CJ0026 - EN:UF and AB v Land Hessen [EB/OL]. [2026-02-14]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0026. UF and AB v Land Hessen.

[25] Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l' uso dei dati biometrici e il monitoraggio degli italiani [EB/OL]. [2026-05-03]. https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751323.

[26] Breach of the Protection Obligation by Marina Bay Sands Pte Ltd [EB/OL]. [2026-05-03]. https://www.pdpc.gov.sg/organisations/regulations-decisions/enforcement-decisions/breach-of-the-protection-obligation-by-marina-bay-sands-pte-ltd.

[27] Ji Leilei. Theoretical reflection and reconstruction of data rights confirmation [J]. Journal of Shanghai University (Social Sciences Edition), 2025, 42(1): 15-29.

[28] Feng Xiaoqing. Property-right protection and institutional construction for enterprise data in the era of big data [J]. Contemporary Law Review, 2022, 36(6): 104-120.

[29] Yang Siying, Wang Minglei. The theoretical logic and practical path of enterprise data rights confirmation in China during the "15th Five-Year Plan" period [J]. Journal of Fujian Normal University (Philosophy and Social Sciences Edition), 2025(6): 21-34.

[30] Mei Xiaying. A theory of enterprise data rights and interests: From property to control [J]. Peking University Law Journal, 2021, 33(5): 1188-1207.

[31] 17-16783 - hiQ Labs,Inc. v. LinkedIn Corporation [EB/OL]. [2026-02-14]. https://www.govinfo.gov/app/details/USCOURTS-ca9-17-16783/USCOURTS-ca9-17-16783-1.

[32] Liu Jianchen. Reflection on and solutions for the protection of enterprise data empowerment [J]. Nanjing University Law Journal, 2021(6): 1-20.

[33] Ding Xin, Fan Yusheng, Cai Chun. An exploration of classified management of enterprise data assets [J]. Friends of Accounting, 2025(24): 68-73.

[34] Santoro C, Chandrasekhar R, Milan S. Open data meets data justice [J]. Internet Policy Review, 2026, 15(1): 1–30.

[35] National Data Administration. *Implementation Specifications for the Authorized Operation of Public Data Resources (Trial)* [EB/OL]. [2026-02-14]. https://www.nda.gov.cn/sjj/zwgk/zcfb/0120/20250120171914419632974_pc.html.

Research on Entitlement Strength Allocation of Data Rights Confirmation

Zhang Xiao1 Liu Zhengming2

(1. School of Economics and Management, Shanghai University of Political Science and Law, Shanghai 201701, China;
2. Human Resources and Social Security Bureau of Qingpu District, Shanghai 201799, China)

Abstract: [**Purpose/Significance**] Against the backdrop of data factorization, chain-based utilization, and cross-context circulation, this paper constructs a differentiated allocation framework centered on entitlement strength, aiming to provide theoretical reference and institutional construction guidance for resolving the dual dilemma of right fragmentation and centralized control. [**Method/Process**] This paper defines data-typed rights confirmation as an institutional generation mechanism, and introduces three law and economics criteria—incentive mechanism, externalities and risk diffusion, as well as institutional frictions—to establish their corresponding relationships with rights structure, behavioral rules and responsibility mechanisms. On this basis, the institutional analysis is conducted along the main line of the differentiated allocation of entitlement strength. [**Result/Conclusion**] Data rights confirmation requires differentiated allocation of entitlement strength and governance instruments according to different data types. Personal data should be subject to strict restrictions and enhanced accountability. Enterprise data should be relatively strengthened while subject to competition constraints. Public data should adhere to minimal exclusivity and rule-based openness.

Keywords: Data rights confirmation; Entitlement strength; Law and economics; Externalities; Institutional frictions

---

(Responsible editor for this article: Wei Jin)

Note: Figure translations are in progress. See original paper for figures.