

About China's Data Rights Confirmation Puzzle: Four-Layer Dynamic Rights and Interests Are Broken

Zhuoer Zhang

*School of Law, Zhejiang Wanli University, Ningbo, China
zhangzhuoer99@gmail.com*

Abstract. In the era of the digital economy, although data is becoming increasingly valuable as a core factor of production, a long-term debate has been ongoing regarding the right definition. Article 127 of the Civil Code of the People's Republic of China protects data ownership rights without explicitly defining them. Academia has produced numerous theories, but these fall short when it comes to addressing complex issues like resolving conflicts between data symbiosis and data monopolization. The paper uses literature review, case study, and normative analysis to reveal the weaknesses of current theories. It then deconstructs the judicial logic behind the first batch of judicial protection of data rights guiding cases released by the Supreme People's Court of China in August of 2025, known henceforth as the guiding cases for "the guiding cases". Based on the above, it establishes four levels of dynamic rights: the "Foundation Layer", the "Core Layer", the "Application Layer", and the "Liability Layer". Also breaks through the traditional way of confirming rights, just like the laws now in circulation, such as the Civil Code and Anti-unfair Competition Law, as well as cross-platform data transfer issues, and so on. Additionally, it addresses the problem of rights after the transformation of uncrossed data. will also be able to provide both the ideological directions and concrete directions for drafting laws on the properties of the data, and make the judges rule on the same issue in the same way.

Keywords: Data, Data Rights, Data Ownership

1. Introduction

With the advent of the third industrial revolution, data has become an important new factor of production that drives economic growth, and its value is getting more and more prominent. April 2020 saw China release "Opinions of the Central Committee of the Communist Party of China and The State Council on Establishing a More Perfect Market- Oriented Allocation System for the Elements of Production". This elevates data to the same status as elements of production like land and capital. The "Twenty Data Measures" were then introduced to form 4 basic systems of data governance and promote their implementation. In 2022, when the expert discussed the data element summit of the Global Digital Economy Conference, he put forward "we take the challenge and situation in the data element market as the starting point for enriching our research on data property rights [1]." A new approach is needed to explore additional paths for the confirmation and authorization of data rights based on a tiered method. We have to improve the system that confirms

and authenticates data property rights. In August 2025, the Supreme People's Court published a guiding case on protecting data rights that adopted different ways to rule depending on different data rights cases due to necessity.

In order to develop a system capable of protecting itself on multiple levels, it is necessary to attribute legal characteristics to data. Due to China's civil code not having specific provisions for data legal characteristics, academia has formed different theories, such as the new property rights theory, Sun Y.Z's intellectual property rights theory, and Wang L.M's theory of competitive interests, to name a few [2,3]. But theory has been bound by the logic of conventional rights systems in a way that makes it prone to single-entitlement verification. Single-entitlement verification does not recognize the nature of data—that it is reproducible, not exclusive, and that the existence of data might have some kind of value.

On a practical level, guidelines for cases acknowledge that data is a new type of thing and has many features that can't be classified using current laws. In a way that is complex, all-encompassing, and finely detailed to require continuous examination if a systematic adjudication framework can be established around the idea of "layered protection of rights, active regulation of behavior, fair balancing of interests", applying the adjudicating logic to settle actual cases and solve actual problems, pointing out that de-emphasizing absolute ownership and emphasizing dynamism is both necessary and possible.

In light of the above context, this paper will analyze the shortcomings of already mainstreamed theories by looking at what data features can't fit into the rights framework. It will then lean on the good points of judicial innovation in the first batch of guiding cases. Finally, it provides a "layered dynamics right system", from which theories of improvement of legislation of data property rights, as well as to unify standards of judicial decision-making making could be drawn on.

2. Data classification defines the reasons for rights and interests

The original push for creating and searching to discover laws was due to dealing with problems and issues that kept appearing in society. It's right to argue about the nature of data rights, as it cannot be resolved by traditional legal methods precisely because of this newborn right born out of data—existing in reality.

The primary goal of legal research should be to address real-world issues, not to chase abstract theoretical neatness or internal coherence. Instead, we ought to construct a rights framework by looking at how rights actually operate when they regulate data-related conduct and when they balance competing interests. A functionalist perspective may offer a more practical route for resolving concrete problems. The reason for layered data rights is that:

2.1. Mainstream theories have limitations

Single-entitlement approach refers to the tendency in legal theory to set the legal property and rights of data by using an entire interpretation and regulation of data rights with one form of entitlement, such as property rights, intellectual property rights, competition rights, and thus ignoring the characteristics of multi-subject, multi-level data rights. The New Property Rights Doctrine says that data is a brand-new kind of property, distinct from a property right or an intellectual property right. it has its own separate property attribute; therefore, a new type of property right must be formed, which is neither the traditional property right nor the intellectual property right. The theory regards data as a single property right, ignoring the many distinctions from traditional rights within it. It also certainly doesn't cover every scene.

2.1.1. The new property rights doctrine

The new property rights doctrine posits that data constitutes a novel civil property object not covered by traditional legal frameworks such as property rights or intellectual property rights. Possessing independent property attributes, it warrants the establishment of a new category of property rights distinct from traditional property rights and intellectual property rights. However, this approach seeks to encompass all data-related rights under a single property right, overlooking the inherent complexity and diversity of data. It clearly fails to comprehensively cover all scenarios, representing an oversimplification of data rights.

2.1.2. Intellectual property argument

The Intellectual Property Argument contends that data, knowledge, and information are essentially the same thing, with only partial differences. Data is a natural extension of intellectual property objects, and data fitting into the intellectual property framework is also a reflection of the inclusiveness and openness seen throughout intellectual property's development [4]. It is clearly inconsistent with the defining characteristics of intellectual property, and therefore, data rights cannot be considered a form of intellectual property. Sun Y.Z. pointed out that "data is a reflection or presentation of facts and possesses no originality in itself. Even if significant intellectual effort was invested in obtaining the data, this fundamental nature remains unchanged (e.g., Einstein's derivation of relativity formulas). Only the intellectual creation involved in selecting or arranging the data may give rise to originality [2]." This doctrine seeks to extend intellectual property protection to simple data collections that are difficult to qualify as intellectual property, exhibiting a tendency toward singular rights confirmation.

2.1.3. Competitive interest theory

The competitive interest theory avoids defining the nature of data and advocates protecting data rights by regulating unfair practices through Articles 2 and 12 of the Anti-Unfair Competition Law [3]. However, the legislative purpose of the Anti-Unfair Competition Law lies not in confirming civil rights but in protecting them. Therefore, it cannot directly establish data-related rules to resolve data rights attribution issues [5]. Furthermore, the rules of the Anti-Unfair Competition Law apply only to disputes involving data between operators in competitive relationships. For disputes arising between non-competitive parties or where one party is a non-operator, the direct application of this law becomes difficult [5]. This doctrine essentially ties the legal attributes of data solely to competitive interests. The theory of competitive interests, which seeks to protect data rights through the Anti-Unfair Competition Law, essentially confines the legal nature of data solely to issues of competitive interests. This approach overlooks the independence and multi-layered nature of data as an object of civil rights, thereby similarly reflecting a tendency toward "single-dimensional rights confirmation."

2.2. Defining rights and interests through data stratification

2.2.1. Facilitates solving practical problems

On one side, the hierarchical definition of right and interests is distributed by different subjects who play the role and make contributions in the data exchange, which can better balance the demands of all parties.

On the other hand, this approach becomes less important to judge who is the "final owner" of the data; however, direct judges are subject to gaining and using data reasonably or unreasonably. For example, such a framework helps assess whether the interests of the original data provider were respected during subsequent uses of the data, and whether anyone has over-extracted value from the labor of others. By working from this perspective, many disputes can be resolved more clearly, which can avoid the unproductive back-and-forth of blanket demands for "exclusive control" or "complete prohibition" that often arise when data is treated purely as a form of property accessible to all.

2.2.2. Facilitates adaptation to social development meanwhile maintaining the legal system

Looking at it in terms of whether something is steady, as for defining how the layers are broken up, things have barely changed for now. Not breaking the civil rights rules or changing big rules like the laws on property or on being fair. Not the contrary of it, data rights are classified according to a certain rule in order that stratification adapts to the present legal protection rules. It is important to supplement and improve the current legal system and maintain the relative stability of the current law. In this way, all the parties involved in the fight get it right on which guideline applies through this layered logic, and can resolve issues as fast as possible.

From an adaptive development standpoint, data stratification permits flexible answers to brandishing scenarios and can modify stratification material as required without amending the law. Beyond Case No. 264, in denying "single ownership" and embracing concurrent data rights, Guiding Case No. 263 addressed cross-platform data transfer disputes [6,7]. Through layered approaches, 'balance platform data management rights and user data portability rights', establishing the circulation principle of 'user authorization + non-disruption of order' to address the practical problem of breaking 'data islands', among no amendments to laws were made in any of these cases. Instead of solving the problems of infringement that data scraping, cross-platform data flow, etc., may cause through the stratification of rights alone. So as not to have a single rights confirmation model to become set in its ways and fall behind the digital economy's development. It is very possible, though it's kind of imperfect.

3. Tiered data rights model

Giun C.L put forward a way to convert the semantic heterogeneity issue into one of "representational diversity", and classified data into four tiers: conceptual layer, linguistic layer, knowledge layer, and data layer [8]. The four-tier dynamic rights structure, consisting of "Foundation Layer-Core Layer-Application Layer-Responsibility Layer," was formulated on the foundation of this concept, with China's specific policy orientation also taken into account.

It does not lead to overly simplified, absolute decisions for the rights of data. Relying on real life makes things easier to solve when it comes to data. This system's protection of the interests of a person as a data subject is scope and level of data protection provided by this system depends on whether it can reach an accommodation between data protection interests and other interests.

3.1. Foundation layer

Put data into 3 groups according to "actual control capability," and set up a voluntary registration system to help with rights definition.

Controlled data refers to information that enterprises can control through encryption, permission settings, and other means. Core Customer Database and owned Modelling Training Set, etc. When controllers are granted a defensive right, they can lawfully protect their control over data from others who might illegally destroy or seize it. In parallel, a unified national data-control rights registration authority is established, allowing controllers to voluntarily register their data control rights over important datasets. The registration records become one of my defenses. The registration records have become a good way to protect oneself. To seize a position of strength by owning data as if issuing a public notice of property rights to lighten the onus of proof and safeguard the rights of people possessing it. About the voluntary registration process: First, submit the required documents via the controller. The registration authority looks at the materials to check if they are complete. It gets a compliance registration certification upon approval, which is then registered in the system and publicly displayed to the public. No registration, and there must be rights that have a controller. Registrations merely give controllers an officially recognized place for keeping track of things, which lets them legally claim exclusive ownership over whatever gets registered without having to fear having something mimicked by someone else. It's like sending out a "red light" signal to all those other users that want any bit of your data that has been registered. Every individual using the above data shall comply with the laws and regulations.

As a kind of "recording authority", it can promote mutual understanding and trust between the parties involved in the data transaction, making the data transaction more efficient.

Holding data happens when those subjects of data don't actually control the data but merely possess a technical right to use it. That is to say, he can take advantage of the data technically and make use of the data for business purposes without controlling the data exclusively and at will. Take the content that users post on social platforms or the consumption content of users—the platform is still storing it, but these contents also give users certain usage rights. Thus, it should be recognized as "holding rights" rather than an old "ownership" idea. Allow the controller to have "defensive rights," so the controller can do whatever is necessary and legitimate to stop unauthorized third parties from damaging the data under its control or just taking it away. At the same time, by establishing a unified national data control-rights registration platform, controllers may voluntarily apply to register control rights over core data. Registration records serve as strong evidence of control over the data. Similar to the public announcement of property rights, the registration of data control rights facilitates easier proof of such rights and provides stronger protection for the parties that exercise control over the data. As for voluntariness of registration procedure: First, the controller submits the online requirement documents.

Registration authority looks for complete info. If a compliance registration certificate is given out and entered into an official system, and publicly disclosed. But it's not missing in order for a controller to have its right to register.

Registration gives controllers official platforms for record keeping and lawful, exclusive exercise over certified data and serves as a "Red Light" warning to any third parties who wish to make use of registered data. Registration creates the controller's official platforms for record keeping and legally exclusive control with respect to certified data, and it is a "Red Light" warning any 3rd parties that wish to make use of registered data.

He M.X noted, "As controlled data, it must be at least two types: controlled data content, controlled data generated by a control method. Neither can be omitted." Based on this approach, data ownership can be identified by examining the data under a party's control and the specific methods used to exercise that control, thereby determining the true holder of the data. In addition, rules safeguarding users' rights to data portability should be established. Platforms cannot prevent

the transfer of data through standard terms and conditions or through cross-platform technical restrictions. prohibitive method should prohibit people who can't be forced to use only one platform because of the fact that the data is unable to move.

The public data can be provided to everyone completely. Following the 20 Data Guidelines, society can gain access to richer data resources, improve overall quality of life, and accelerate the development of industries that rely on data.

3.2. Core layer

To solve the trouble that accurate distribution of rights and interest can be realized through a quantitative method when a piece of data is co-created among lots of people, this system will create a corresponding traceable and enforceable one. Wang L.M said: "Data generation, data collection, data cleansing, data tagging, data processing, data storage, data usage rights between data originators and data processors should follow the principle of identifiable work and shareable benefits, storing all evidence of data circulation with the help of technology such as block chain [9]." To ensure full process evidence storage of data circulation, the contribution ratios of each participant during the entire data life cycle, generation, data collection, data cleaning, data tagging, data processing, data storage, and data use must be determined, which requires the implementation of a contribution recording principle throughout the entire data flow process. It's about noticing – like who joined in and the effort someone put in, and then what came out when the data went on a little ride around. Using this approach can turn the data flow process into trackable events with an event log, so as to deal with the problem of following fast-moving data. It makes people get a fair record of distribution. It becomes evidence as well if there are disputes as far as it is concerned.

By tallying contributions made and amounts owed by all parties at each stage, quantifying these figures, and allocating proportions accordingly, benefits can be distributed among different stakeholders with clear delineation of entitlements. Number two, they can also use this type of observation record as evidence to support their judgment, so that it can make their judgment more fair and unbiased and fair.

This mechanism can visualize each individual's participation and truthfully record the entire data flow, thereby preventing any party from monopolizing benefits.

3.3. Application layer

Because every real-world scenario is going to be slightly different from another so the risk data products also have to be different with characteristics as well. Therefore, it is necessary to make the system flexible. The Personal Information Protection Law stipulates a notification and consent model, and also conducts a dynamic model of informed consent. Each time the data utilization purposes change and every time crossing various scenarios for their usage, the data users will need to acquire fresh consent authorizations. Users withdraw to when platforms comply with the Standard Contract for Cross-border Transfer of Personal Information, and delete personal information or anonymize it after 15 days of withdrawal to conform with the requirements of data deletion or anonymization.

The platform should employ an irreversible encryption algorithm to delete this data. It should be destroyed, and the evidence provided to demonstrate deletion, so regulators can continue to destroy.

The second, try to set up trial projects in risky sectors like the digital economy / smart cars/healthcare Company will give over to a risk contingency plan, regulatory body will do so in real time. Violate and it'll be suspended for correction straight away. Wells used FAIR–AI methodology,

which can also be employed by China's AI medical trials - an interdisciplinary review committee comprising physicians, data scientists, and ethics professors, and a four-dimensional evaluation rubric including validation, utilitarianism, transparency, and fairness to make it quantifiable and trackable [10]. This will make room for new forms of action – as with the use of AI algorithms in medicine – without letting go of our safety standards.

3.4. Responsibility layer

Clarify the upper limit and the responsibility mechanism for the exercise of the right to avoid abuse. All data processing should follow the principle of "mini necessity," which requires enterprises only to collect and process necessary data and avoid excessive collection. Concerning the matter of doing data safeguard procedures, firms have to run regular safety inspections together with intrusion testing, also correct known security flaws. If the data is due to the enterprise not having made a reasonable protection measure. The fault shall be punished according to the law and according to the scale and extent. Therefore, noting that down in the credit file according to the regulations. If an enterprise uses operating rights to monopolize data, the regulatory department shall find out the market share of the data and the scope of control of the enterprise. Referring to Article 57 of the antimonopoly Law, to impose a fine of 10% of the sales of the enterprise in the last year. At the same time, relief measures should be introduced, such as open databases, splitting data, services, etc. The European Commission investigating the anti-monopoly case of Amazon, the European Commission stipulated that Amazon should enhance its usage of third-party seller data, vowing not to utilize non-public business data from third-party sellers anymore for its internal operations, thus averting a data monopoly [11]. These kinds of remedial safeguards are worth referring to.

In short, this framework adopts a comprehensive four-layer classification that includes the foundations layer, the main body parts layer, the applying layers, and the accountability layer to deal with lots of real-world situations and change it according to the characteristics of the data to create a brand new and reasonable way that will improve data management systems.

4. Conclusion

This paper finds through analysis that there is a "one-time right of confirmation" phenomenon in the current data rights theories. This leads to the theory being unable to solve real problems: Data is an object consisting of expansive and fluid rights bearers of rights. Therefore, one single right does not cover all the rights that are data. And even worse, the data is messy and tangled, and only having one entity own the data does not allow people to share data, the data to be circulated, and the value of the data cannot be realized. And it also increases social costs and ultimately destroys the data industry chain. Expanding the logical rules of leading cases to establish a layered and dynamic protection system for rights can push forward in the constant progress of legal system improvement and growing under the current Chinese legal system. It can help to create more complete laws and regulations for data, which will make it clear to judicial practice who has the right to data, and thus make fair and just determinations of data disputes.

For example, in a hospital that uses tiered dynamic rights management on different types of medical data, for example, it could be categorized into 3 types of data: data controlled by people, hospital data, and medical research. It's important for the hospital to decrypt related patient data before it is added to the experimental research database.

Even though authorized, the concerned departments should continuously supervise things to maintain the patients' privacy and allow the medical industry to develop. but also in the areas of

cross-border data coordination and the coordination of rights and interests.

Future endeavors ought to be spent researching how best to rule over data that straddles boundaries, making sure those theories about the matter align with how people utilize it, so such theories can better tackle actual issues that judges confront when ruling on what the law stipulates.

References

- [1] Zheng J.N (2021). Exploration of the Legal Attributes of Data and Information Property, *Oriental Law*, No. 5, pp. p43-56
- [2] Sun Y.H, (2021). Combining and Referring to Data Protection in the United States and the European Union, *Political and Legal Reviews*, Vol. 04
- [3] Wang L.M, (2023). How to Confirm Data Rights, *Legal Research*, Vol. 45, No. 04
- [4] Dong T, (2025). Research on the Legal Attributes of Data Property Rights under the Historical Evolution of Intellectual Property Rights, *Comparative Law Research*, Vol. 03
- [5] Cui G.B, (2019). The Basic Theory of Limited Exclusivity in Big Data, *Legal Research*, No. 5.
- [6] Shanghai No. 2 Intermediate People's Court (2023). Hu 02 Min Zhong No. 11028 Civil Judgment. <https://ipc.court.gov.cn/zh-cn/news/view-4588.html>
- [7] Shanghai Intellectual Property Court (2019). Hu 73 Min Zhong No. 263 Civil Judgment. <https://ipc.court.gov.cn/zh-cn/news/view-4588.html>
- [8] Giun C.G, F., Zamboni, A., Bagchi, M., & Bocca, S. (2021). Stratified Data Integration. arXiv: 2105.09432.
- [9] Wang L.M. (2023). On the Rights of Data Sources, *Legal System and Social Development*, Vol. 29, No. 6
- [10] Wells, B. J., et al. (2025). A Practical Framework for Appropriate Implementation and Regulation of Artificial Intelligence in Healthcare. *npj Digital Medicine*, 8(1), 1900.
- [11] European Commission. (2022, Dec 20). Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime. Brussels: European Commission, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777