Выбор моделей и институциональное построение для выполнения фидуциарных обязанностей доверительного управляющего данными

The Selection of Models and Institutional Construction for Fiduciary Duties of Data Trustee

Ду Цишунь,
доктор юридических наук, доцент юридического факультета
Хэнаньского университета, Кайфэн, КНР
e-mail: duqishun@126.com

Дай Юйхань,
исследователь Китайско-российского центра
сравнительного правоведения
Хэнаньского университета, Кайфэн, КНР
e-mail: 2215382355@qq.com

Du Qishun,
Doctor of Law, Associate Professor
at the Law School of Henan University, Kaifeng, China
e-mail: duqishun@126.com

Dai Yuhan,
Research at Chinese-Russian Center for
Comparative Law at Henan University, Kaifeng, China
e-mail: 2215382355@qq.com

DOI: 10.17803/2587-9723.2025.8.021-026

Аннотация. *Являясь институциональной инновацией, возникшей в результате взаимодействия механизмов защиты данных и доверия, data trust демонстрирует значительный потенциал в эпоху больших данных, одновременно бросая вызов традиционным механизмам фидуциарных обязательств. Существуют две модели доверия к данным: американская модель теории информационного доверия и британская модель доверия к данным. Китай мог бы принять гибридную операционную модель доверия к данным, при которой доверитель и попечительское лицо устанавливают отношения доверия к данным посредством соглашения о доверительном управлении. Трастовая компания выступает в качестве доверительного управляющего для выполнения фидуциарных обязанностей, в то время как государственные регулирующие органы осуществляют надзор за операциями по доверительному управлению данными. Согласно этой модели, трастовая компания и пользователи данных являются основными субъектами, ответственными за выполнение фидуциарных обязанностей.*
В дополнение к обязанностям лояльности фидуциарные обязанности должны также включать обязательство обеспечивать безопасность данных доверителя, способствуя при этом полному распространению данных для реализации их ценности как актива. Когда учреждение, доверяющее данные, нарушает свои фидуциарные обязательства, бремя доказывания переходит к доверенному лицу и применяется принцип предполагаемой ответственности. Кроме того, специальный регулирующий орган должен установить лицензионные требования для учреждений, доверяющих данные.
Ключевые слова: *доверие к данным, доверительный управляющий данными, фидуциарные обязанности, обязательства по защите данных*

Abstract. *As an institutional innovation emerging from the interplay between data protection and trust mechanisms, data trust demonstrates significant potential in the big data era while simultaneously challenging traditional fiduciary duty frameworks. There are two models of data trust: the U.S. "information fiduciary theory" model and the UK's "data trust" model. China could adopt a hybrid*

operational model for data trust, where the trustor and trustee establish a data trust relationship through a trust agreement. The trust company acts as the trustee to fulfill fiduciary duties, while public regulatory authorities oversee data trust operations. Under this model, the trust company and data users are the primary entities responsible for fulfilling fiduciary duties.
In addition to duties of loyalty and care, fiduciary duties should also include the obligation to ensure the security of the trustor's data while promoting the full circulation of data to realize its value as an asset. When a data trust institution breaches its fiduciary duties, the burden of proof shall shift to the trustee, and the doctrine of presumed liability shall apply. Additionally, a dedicated regulatory authority shall establish licensing requirements for data trust institutions.
Keywords: *data trust, data trustee, fiduciary duties, data security protection obligations*

1. Introduction

Data is the core production factor that drives the construction of Digital China and accelerates the development of the digital economy. In the era of data economy, phenomena such as data leakage and abuse continue to emerge, and the traditional "empowerment rights protection" model is difficult to achieve effective data governance. The contradiction between data protection and data circulation and utilization is gradually intensifying. As a product of the interaction between data protection and trust mechanisms, data trust has shown great potential for application and has gradually become an important direction for global data governance reform. Overall, at present, China's "data trust" only borrows the concept of trust, and some issues related to data ownership and trust theory in data trust have not yet been resolved. Traditional fiduciary duties are grounded in the framework of property trusts. However, the unique attributes of data — including its intangible nature, replicability, and platform dependency — pose systemic challenges to conventional fiduciary models. These challenges manifest in three key dimensions: First, the ambiguity of data ownership undermines the legal foundation for determining trust property; second, the involvement of multiple parties in data processing obscures the identification of fiduciaries; third, traditional fiduciary duties such as the duty of loyalty and duty of care require expansion to incorporate at minimum a duty of security. The limitations of traditional fiduciary obligations necessitate the development of a new fiduciary framework adapted to data's unique characteristics, for which comparative jurisdictional practices provide valuable reference.

Currently, there are two distinct models of data trust: The U.S. "information fiduciary theory" model, which imposes strict fiduciary obligations on data processors. The U.K. "Data Trust" model, which establishes independent third-party institutions to provide data trust services. These two models are not mutually exclusive regulatory approaches — each has its own institutional strengths and weaknesses, and their effectiveness often depends on contextual application in specific scenarios. Based on comprehensive consideration, China can adopt a hybrid operation mode of data trust, that is, the trustor and the trustee establish a data trust relationship by signing a trust contract, the trust company performs its fiduciary obligations as the trustee, and the public regulatory department implements data trust supervision. Therefore, it is necessary to build the system with the trustee's obligations as the core. Specifically, it is necessary to clarify the subject who bears the fiduciary obligation, expand the content of the fiduciary obligation to cover the requirements of data security, compliance sharing and algorithm transparency, improve the accountability mechanism, introduce the inversion of the burden of proof to reduce the burden of proof on the trustor, establish the access standards and dynamic supervision system of data trust, and take the fiduciary obligation as the constraint framework to promote the realization of the dual functions of data trust in protecting personal rights and interests and promoting data circulation.

2. The impact of data trust on traditional fiduciary duties introduction

Data trust maintain the orderly development of the data trading market by drawing on the trust's fiduciary mechanism. Traditional fiduciary obligations are built based on property trusts. Faced with the characteristics of non-material data, replicability and platform dominance, the traditional normative model faces systematic impact.

2.1. Challenges to data as trust property

Whether data rights can become the property of trusts is a controversial issue since the idea of data trust was put forward. Article 11 of the Trust Law of the People's Republic of China (hereinafter the Trust Law) stipulates that the trust is invalid when "the trust property cannot be determined". Trust property must be property whose value can be determined, but China has not made a clear definition of the ownership of personal data at the legislative level. Article 127 of the Civil Code of the People's Republic of China (hereinafter the Civil Code) adopts induced clauses for data protection, stipulating that

data and network virtual property are objects of civil rights, and does not clarify their rights attributes. In December 2022, The State Council of the People's Republic of China released the "Opinions on Establishing Foundational Data Systems to Maximize Data Element Utilization" (hereinafter the Data Twenty Provisions). This document proposes to explore the structural division system of data property rights, establish a data property right system framework of "three division" of data resource holding rights, data processing and use rights and data product management rights, emphasize the right to use data, but does not stipulate the ownership of data. The Data Security Law of the People's Republic of China (hereinafter the Data Security Law) has made general provisions on data trading and data trading institutions. In fact, "the data are not recognized as property that the trustee can lawfully own and therefore require significant amendments to the trust law".

2.2. The subject of fiduciary duty in data trust is not clear

In the legal framework of data trust, the identification of the subject of fiduciary obligations is faced with structural difficulties. According to the provisions of Article 2 of the Trust Law, the entrusted subject should have clear property management authority and legal status. However, the special nature of data elements makes it difficult to directly apply this determination standard. On the one hand, data resources are highly concentrated in digital platform enterprises, which have formed "Data Power", but their legal status as potential trustees has not yet been clarified. On the other hand, the multi-stakeholder structure emerging from data property rights partitioning mechanisms — comprising data holders, data originators, and data users — endows fiduciary duty bearers with inherent composite characteristics. Specifically, although data holders, as "de facto controllers," are at the core of data circulation, their rights are limited by the Personal Information Protection Law of the People's Republic of China (hereinafter the Personal Information Protection Law). data originators, as the initial rights holders, often lack actual control. Data users, on the other hand, face difficulties in determining responsibility due to differences in access channels. This structural misalignment between subjects, rights, and responsibilities makes it difficult to establish a stable chain of fiduciary relationships in data trust.

2.3. The content of traditional fiduciary duty lags behind

Traditional fiduciary duties consist of the duty of loyalty and the duty of care. The duty of loyalty requires trustees to avoid conflicts between their personal interests and those of beneficiaries. The duty of care obligates trustees to act diligently and prudently in executing entrusted matters. In the context of data trust relationships, trustees must not only fulfill these traditional obligations but are also subject to enhanced fiduciary duties — specifically, a strict duty to promote optimal interests. In addition, the trustee shall also assume the obligation to promote the full flow of data to realize the value of the data property while ensuring the security of the trustor's data. Measures to ensure data security, such as classified and hierarchical protection of data, notification of data leakage and remedial measures, have become the new fiduciary obligations of trustees under the data trust theory. Therefore, the contents of traditional fiduciary obligations cannot meet the needs of data security and circulation under the data trust mode, and updating the contents of fiduciary obligations has become an inherent meaning to promote the development of the data trust mode. Therefore, the contents of traditional fiduciary obligations cannot meet the needs of data security and circulation under the data trust mode, and updating the contents of fiduciary obligations has become an inherent meaning to promote the development of the data trust mode.

3. Two models of fiduciary duties in data trust and their selective application

Data governance constitutes a comprehensive regulatory paradigm. A critical imperative lies in objectively evaluating the U.S. "information fiduciary theory" and the U.K. "data trust" framework, thereby establishing theoretical foundations for developing China's distinctive data trust practice.

3.1. Two models of fiduciary duty in data trust

3.1.1. The U.S. "information fiduciary theory"

The Information Fiduciary Theory, proposed by Professor Jack Balkin of Yale Law School in 2016, posits that technology companies that hold user data in the digital age should be recognized as new fiduciary duty entities. When technology companies collect and process users' personal information, provide professional services, or when users have a reasonable reliance on them, they should assume fiduciary duties of loyalty and care like those of traditional fiduciaries. This theory innovatively extends fiduciary legal relationships from traditional fields such as finance and healthcare to digital platforms, providing a new legal basis for regulating the data power of technology companies. In terms of specific application, the theory emphasizes that the identity of the information trustee should be determined based on two key elements, namely "power asymmetry" and "reasonable trust," rather than being confined to the formal requirements of traditional trusts.

3.1.2. The Theory of Third-Party Data Trust in the U.K.

The trust system originated in Britain, but Britain has developed a completely different theory of data trust — the third-party data trust model. In 2014, Sean McDonald first proposed the creation of a trustee organization holding the underlying code and data generated by technology. Subsequently, the British Government published the Report on Developing the Artificial Intelligence Industry in the United Kingdom in 2017, which considers that data trusts are a series of relationships established to ensure that data is shared in a fair, safe and equitable manner. As the operational manager of the data, a data trust is an entity entrusted with certain responsibilities, designated to hold a number of "trusts" on behalf of a specific group of beneficiaries to protect the interests of users, such as supervising the use of data according to the authority granted by users, and planning to share data with third parties according to the purpose of establishing a data trust.

The above are innovative solutions to the challenges in data management in the digital age. Their common point is to try to protect the rights and interests of data subjects by restricting the rights of data controllers, to adjust the power asymmetry in data circulation. However, the United States information fiduciary theory also faces many controversies, such as possible conflicts with the freedom of speech protected by the First Amendment to the United States Constitution, and practical difficulties such as how to balance commercial interests with user rights and interests. Opponents of the British third-party data trust theory argue that there is an inherent conflict between the fiduciary duties that such data companies owe to data subjects and the fiduciary duties under company law. Furthermore, from a cost-benefit perspective, treating fiduciary duties as a data protection mechanism is not an economical strategy.

3.2. The selection and application of data trust operation models in China: hybrid data trust operation models

The discussion on the fiduciary duty system of data trustees in China shows a pattern of dualistic division, some support the third-party subject as the data trustee under the data trust mode, and some support the data processor as the data trustee under the information fiduciary theory trustee mode. What should be clarified is that they are not two mutually exclusive institutional models, each of which has its own advantages and disadvantages, and often needs to be applied according to specific circumstances to give full play to the real institutional effect. Based on comprehensive consideration, China can adopt a hybrid operation mode of data trust, that is, the trustor and the trustee establish a data trust relationship by signing a trust contract, the trust company performs its fiduciary obligations as the trustee, and the public regulatory department implements data trust supervision. The hybrid operation mode of data trust has obvious advantages: First, it establishes a trust relationship between the trustor and the trustee by signing a contract, which effectively guarantees the data rights. Second, trust companies can effectively engage in data trust business. Third, public regulatory agencies can deal with violations of laws and regulations on data trust in a timely manner to maintain the trust market environment. Under effective supervision, personal data controllers can reasonably manage and dispose of trust data, attract more data subjects to participate in it, and form a virtuous circle mechanism in the data trust market.

4. The institutional architecture of fiduciary obligations in data trust regimes

4.1. Fiduciary duty bearers in hybrid data trust model

4.1.1. The data trust company is the direct undertaker of fiduciary obligations

In the hybrid operation mode of data trust, the data holder shall establish trust according to the data assets owned by himself, and the trust company shall transfer, dispose of, trust and operate the data assets for the benefit of the beneficiary in the name of the trustee. There is nothing wrong with trust companies assuming direct fiduciary obligations in this process. First of all, from the analysis of subject qualification, only licensed trust companies have the legal qualification to establish and operate trust products in China. At the same time, the trust company's long-term professional experience in asset management naturally meets the complex needs of data asset management, providing capacity guarantee for its performance of data fiduciary obligations. Secondly, trust companies are at the core of the data trust legal relationship. The data assets are regarded as trust property, and the trust company is regarded as the trustee. The operation of the whole data trust is carried out with the trust company as the center. Thirdly, as the direct controller of data assets, the trust company is the primary responsible person for the safety of data circulation, and this responsibility attribute requires the trust company to become the direct subject of performing the fiduciary obligations. Finally, from the perspective of the operating mechanism, the professional competence of trust companies is the key guarantee for the realization of data value. From the custody and operation of data assets to the distribution of final income, the standardized operation of the whole process relies on the professional service ability of trust companies. The combination of these advantages makes the trust company an ideal subject to assume fiduciary obligations.

4.1.2. Data users are limited fiduciary duty bearers

As a trustee, the data user has certain control over the property rights of personal information. Although individuals are not the main contributors to the property value of personal information, in order to encourage individuals to continuously provide personal information, individuals should be included in the scope of personal information sharing. Personal information often exists on the platform, and the form of giving full play to its value is relatively special. Without the collection and processing of data users, the property value of personal information will be difficult to give full play to, thus deciding that the property value of personal information cannot be exclusive to individuals but should be shared by data users and data processors. For enterprise data, enterprises should not be granted absolute exclusive property rights, otherwise the development of the Internet industry may be inhibited. Therefore, data users should assume the fiduciary obligation to assist in the operation; In different data trust products, the same data user may, as different trustors or trustees, bear limited fiduciary obligations, which are required by the duty of care. In a data trust, the trustee shall adopt various ways and means to maintain the security of trust data so as to achieve the purpose of data sharing and utilization in line with the trust. Under the data trust mode, the co-trustees shall supervise each other and jointly maintain the stable operation of the data trust mode.

4.2. Expanding the scope of fiduciary duties in data trust

The fiduciary duty of data trust also includes the duty of prudence and the duty of loyalty, and each duty has different requirements. On the basis of traditional duty of care and duty of loyalty, the fiduciary duty system in data trust must be incorporated into the security obligation as the third dimension to form a complete obligation framework. Security obligations require data trust to maximize the protection of the dignity, privacy and other personal interests of data source subjects. The basis for the circulation and utilization of data is that the personal rights and interests contained in the data will not be infringed, that is, the connotation of data security. The Data Security Law stipulates that the key to data governance, development and utilization is data security. Trust companies have greater authority to manage and use data based on the trust of data subjects, and trust companies should match differentiated protection measures according to the sensitivity of data in trust contracts. Such fiduciary obligations at the security level are not only a result-oriented complement to the statutory obligations in the Personal Information Protection Law and the Data Security Law, but also a private law representation of the personal data security obligations.

4.3. Civil liability for breach of fiduciary duty in data trust

4.3.1. Clarifying the criteria for determining data trust liability

The Personal Information Protection Law adopts the principle of fault presumption. According to the above-mentioned fiduciary obligations of the data trust trustee, when determining that the data trust trustee violates the fiduciary obligations, it is necessary to clarify what fiduciary obligations have been violated, whether actual damage results have been caused, whether there are subjective faults, whether remedial measures have been taken, whether the exemption conditions have been met, and how to compensate, which should become the criteria for determining the liability of the data trust trustee.

4.3.2. The application of reversed burden of proof rules shall govern liability determinations

In general infringement, the infringed person shall bear the burden of proof for the facts of infringement, the consequences of damage, causal relationship and subjective fault. However, in the context of the data trust model, because the data trustee has been given a reasonable legal status, the infringed individual is often unable to collect evidence to prove the relevant facts, and if they are required to bear the burden of proof, they are likely to bear the consequences of losing the lawsuit because they cannot provide evidence. The Personal Information Protection Law "stipulates that the burden of proof of the fault element shall be borne by the personal information processor, that is, the actor who infringes upon the rights and interests of personal information, which belongs to the inversion of the burden of proof".

Therefore, when the personal information right is infringed, the rule of inversion of the burden of proof shall be adopted, and the data trustee may be exempted or mitigated from the tort liability after assuming the burden of proof such as subjective no fault and having taken protective measures for data security. The inverted burden of proof rule can not only balance the litigation status of the infringer and the infringed, but also enable the personal information controller to take stricter measures to protect personal data information in this way, which plays an important role in promoting the realization of fairness and justice, highlighting the rule of good law, and maintaining the normal data trading and sharing market.

4.4. Establish an admission and supervision mechanism for data trust institutions

Not all third-party institutions can qualify as data trust institutions. The establishment and evaluation of such institutions rely on government regulation and market oversight. On one hand, since data trust institutions store a large volume of data information,

their operations must be conducted under the supervision of the national cyberspace administration. During the establishment phase, trust institutions must meet regulatory authorities' qualification requirements to obtain operational approval; during the operational phase, trust institutions must establish dedicated data security management departments, designate a primary data security responsible party, conduct regular risk assessments, and submit assessment results to regulatory authorities. On the other hand, the supervisory role of market reputation mechanisms must be leveraged. The immediacy and low barriers to entry in online communication amplify the role of reputation mechanisms in data market governance. Therefore, in the data trust sector, market entities themselves serve as the best witnesses to determine whether trust institutions have fulfilled their duty of care and loyalty.

5. Conclusion

Data trust, as an emerging model for protecting data rights, emphasize the fiduciary duties of data trustees under the fiduciary law framework, ensuring the reasonable use of data and the protection of data subjects' privacy rights. This new data governance solution provides an effective means of balancing data privacy protection and reasonable data use and is expected to become an important model in the field of data protection in the future. The importance of fiduciary duties in the field of data protection will also become increasingly prominent. However, for the data trust to truly become a cornerstone of China's digital economy governance system, there are still many practical challenges that need to be addressed. For example, while the hybrid operation model of data trust can establish the ownership of data rights through contractual agreements, the legal framework has not explicitly defined the eligibility of data as trust property. Additionally, under the current framework of the three-rights separation of data property rights, while trust companies and data users are subject to fiduciary duties, do data holders and data processors also need to assume corresponding fiduciary responsibilities? If these entities are also required to assume such obligations, could this lead to an unlimited expansion of fiduciary duties? It is foreseeable that the fiduciary duties of data trustees will become an important institutional safeguard for building "digital trust" and promoting the sustainable development of the digital ecosystem.

REFERENCE

1. *Balkin J. M.* Information Fiduciaries and the First Amendment // UC Davis Law Review. — 2016.
2. *Ding Xiao-Dong.* On the Legal Protection of Enterprise Data Rights: An Analysis Based on the Legal Nature of Data // Legal Science (Journal of Northwest University of Political Science and Law). — 2020. — № 2.
3. *Feng Guo, Yan Hao-Yu.* Theoretical Interpretation and Institutional Approach to Fiduciary Duties of Data Trustees // Finance and Law. — 2024. — № 2.
4. *Li Zhi, Yao Tian-Tian.* The Regulation of Trustee's Fiduciary Duty in Data Trust Model // Academic Exchange. — 2022. — № 2.
5. *Li Zhi, Zhou Zhi-Hao.* The Development Dilemma and Institutional Design of Personal Data Trust // Academic Exchange. — 2024. — № 8.
6. *Lu Da.* A Study on the Jurisprudential Interpretation, Generative Logic, and Institutional Construction of Personal Data Trust // Credit Reference. — 2025. — № 1.
7. *Richards N. M., Hartzog W.* Taking Trust Seriously in Privacy Law // Stanford Technology Law Review. — 2019.
8. *Tian Ao-Ni.* Third-party Data Trust: The Dilemma and Solution of Data Controllers' Obligations // Library Tribune. —2022. — № 8.
9. *Wang Li-Ming.* Civil Law Protection of Data // Digital Law. — 2023. — № 1.
10. *Xi Yue-Min.* Data Security: The Purpose of Data Trust and Its Realization Mechanism // Law Science Magazine. — 2021. — № 9.
11. *Xie Zheng-Shan.* Data Privacy Protection in the Data-Driven Era: From Individual Control to Fiduciary Duty of Data Controllers // Studies in Law and Business. — 2020. — № 2.
12. *Xing Hui-Qiang.* Theoretical Challenges to the Fiduciary Duty of Data Controllers // Law and Social Development. — 2021. — № 4.
13. *Yang Li-Xin.* Civil Liability for Infringement of Personal Information Rights by Personal Information Processors // Journal of National Prosecutors College. — 2021. — № 5.
14. *Zhai Zhi-Yong.* On Data Trust: A New Approach to Data Governance // Oriental Law. — 2021. — № 4.
15. *Zhou Han-Hua.* The Legal Orientation of Personal Information Protection // Social Science Digest. — 2020. — № 8.