WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 10, Number 1, Year 2026
DOI: https://doi.org/10.62051/ijsspa.v10n1.05
Journal homepage: https://ijsspa.org

The Chinese Path to Mandatory Data Sharing among Platform Enterprises: A Perspective on the Localized Reconstruction of the Essential Facilities Doctrine

Ke Li

Law School, Jinan University, Guangzhou, China

ABSTRACT

The deepening development of the digital economy has endowed critical data with significant infrastructural properties. However, the "walled gardens" constructed by dominant platforms through "data feedback loops" have increasingly become structural barriers to fair market competition. Against the backdrop of China's "Data Twenty Measures," which established the separation of data property rights, and the amendment of the Anti-Monopoly Law, the mechanical application of the traditional Essential Facilities Doctrine (EFD) faces dilemmas regarding innovation suppression and ambiguity in definition. This paper constructs a regulatory paradigm of "mandatory sharing," predicated on the logic of opening data as a "quasi-public facility." By introducing a tripartite criterion consisting of "ecological non-substitutability," "public necessity," and "technical interoperability," this study reconstructs the constituent elements of essential data. Furthermore, based on the source of value and competitive attributes, it constructs a classified and hierarchical mechanism where "basic operational data" is subject to mandatory sharing in principle, while "derivative value-added data" is exempted in principle. The research demonstrates that establishing a pricing system based on FRAND principles and a "penetrating" algorithmic supervision mechanism can not only break the monopolistic loop of "data feudalism" but also effectively protect innovation incentives through trade secret defenses. This approach offers a distinct institutional scheme with Chinese characteristics for global digital market governance.

KEYWORDS

Essential Data; Essential Facilities Doctrine; Mandatory Data Sharing; Antitrust Law; Interoperability.

1. INTRODUCTION

As the digital economy advances into a deeper phase of development, data has transcended its role as a mere commercial resource to become a core factor of production driving economic growth. Particularly in China, with the promulgation of the "Data Twenty Measures" (officially the Opinions on Building Basic Systems for Data) and the promotion of market-oriented reforms for data elements, the infrastructural property of data has become increasingly prominent [1]. However, accompanying the release of data's public value is the exclusionary control over critical data by dominant platform enterprises. Relying on first-mover advantages and network effects, super-platforms have constructed rigorous "Walled Gardens," alienating data elements-which should be circulating freely-into private barriers that consolidate their monopoly status [2].This tendency towards "Data Feudalism" not only prevents small and medium-sized enterprises (SMEs) from entering the market through innovation due to "data poverty," but also distorts the competitive logic of the digital market from "efficiency priority" to "zero-sum gaming," causing significant efficiency losses and innovation suppression.

Faced with this dilemma, breaking data monopolies and achieving interoperability of critical data has become a common challenge for antitrust laws globally. The traditional Essential Facilities Doctrine (EFD) was once regarded as a potent tool for breaking monopolies in physical infrastructures. However, when transplanted to data-an intangible asset-it faces theoretical challenges, including ambiguous standards of identification, potential dampening of investment incentives, and difficulties in adapting to the non-rivalrous nature of data. Especially against the backdrop of U.S. antitrust jurisprudence tending towards conservatism regarding the EFD (as seen in Trinko), it is particularly urgent for China-a jurisdiction with the world's largest digital application market-to explore a data governance path adapted to local industrial characteristics within the framework of the amended Anti-Monopoly Law [3].

This paper argues that the key to resolving these issues lies in constructing a new regulatory paradigm of "Mandatory Sharing." The core of this paradigm is to recognize the quasi-public attribute of critical data as "new infrastructure." Under the premise of protecting the legitimate rights and interests of data controllers, antitrust law should grant competitors reasonable access and interoperability rights through mandatory force. This is not an unwarranted erosion of private corporate rights, but a correction and return to the essence of "freedom of competition" in the digital economy era.

Based on this, this paper intends to use the localized reconstruction of the EFD as an entry point to explore the following core questions: First, in the context of the separation of property rights established by the "Data Twenty Measures," how should the legal connotation of "Essential Data" be redefined? Second, how can a classified and hierarchical sharing mechanism be constructed that breaks monopoly barriers while effectively protecting trade secrets and innovation incentives? Third, how can a cost compensation and remedy system be designed that aligns with China's enforcement practices? By answering these questions, this paper aims to provide a forward-looking institutional scheme for the rule-of-law governance of China's digital market.

2. COMPETITIVE DISTORTION AND GOVERNANCE DILEMMAS UNDER DATA BLOCKADE

The rapid development of the digital economy has reshaped the fundamental logic of market competition. As a key factor of production, the connotation of data has far exceeded the scope of traditional commercial resources. Under the combined effects of two-sided markets and network externalities, data has gradually mutated into a critical gateway determining market entry and competitive success. When dominant platform enterprises establish unshakable data advantages through long-term user accumulation and algorithmic iteration, such advantages are no longer limited to a single lead in market share but transform into structural barriers hindering fair market competition.

2.1. Market Structure Solidification Caused by "Data Feedback Loops"

The primary impact is the solidification of market structure and non-contestability caused by data feedback loops. Unlike the economies of scale based on physical assets in the traditional industrial era, competition in digital markets exhibits significant self-reinforcing characteristics, known as the "Data Feedback Loop." Large platforms accumulate massive initial data through first-mover advantages and use this data to train and optimize algorithmic models, thereby significantly improving service quality and user experience. This optimization of experience, in turn, attracts more users, generating an even larger scale of data increments. This cyclical feedback mechanism causes data resources to rapidly concentrate towards the head, forming a "Matthew Effect" where the strong get stronger [4].

For late-coming competitors, this mechanism constitutes a dual barrier to entry: one is the barrier of data scale, and the other is the algorithmic barrier derived from data scale. Even if new entrants possess more advanced algorithmic architectures or highly disruptive business models, they cannot

effectively form market supply if they lack the key data support required for a "Cold Start"—such as deep user social relationship chains, cross-scenario historical transaction graphs, or high-precision geographic location information [5]. From the perspective of antitrust law, data at this stage is no longer a purely private competitive asset but has substantially transformed into an indispensable infrastructure for the relevant market. If this barrier is not broken through a mandatory sharing mechanism, the market is extremely prone to falling into a permanent solidified state of "Winner-Takes-All," where potential competitors are completely excluded from the market, leading to a fundamental failure of the competitive mechanism [6].

2.2. Cross-Market Dominance Transmission under the "Leverage Effect"

More concealed and fatal harm lies in the transmission of cross-market dominance and the abuse of leverage effects. Relying on absolute control over basic operational data, super-platforms are often able to engage in leveraging monopoly behaviors, extending their dominant position in the upstream market to adjacent or downstream markets. [7] This cross-border transmission mechanism is particularly prominent in the digital ecosystem: platforms controlling underlying data such as search records, operating systems, or social networks essentially master the traffic gateways and infrastructure of the digital economy. They can hinder competitors in vertical fields (such as vertical e-commerce and local life service providers) from obtaining the data resources necessary for business operations by refusing to open data interfaces, degrading interoperability quality, or setting technical obstacles.

This refusal of access enables platform enterprises to use data advantages to implement self-preferencing. On the one hand, they provide full, real-time data support for their own affiliated businesses, implementing precise asymmetric competitive strikes (often termed "dimensionality reduction attacks" in the Chinese context); on the other hand, they implement data shielding or discriminatory downgrading against independent third parties, artificially raising the operating costs of competitors. This transmission of cross-market dominance causes originally potentially vibrant adjacent markets to shrink rapidly, leading to the degeneration of innovation in the entire digital ecosystem from pluralistic competition to "vassals of giants," seriously destroying the fair competition market order. Behind the seemingly abundant application choices, consumers are actually locked into closed ecosystems constructed by a few giants, and in the long run, will have to bear the bitter fruit of declining service quality and price discrimination.

2.3. The "Dual Suppression" Dilemma of Investment and Innovation

Furthermore, data blockades have created a profound chilling effect in the fields of investment and innovation, forming so-called "Kill Zones" for innovation. Although traditional antitrust theory worries that mandatory sharing may suppress the investment willingness of data controllers, in the current digital oligopoly landscape, the suppression of innovation by refusal to share is more severe and urgent. Due to the lack of core data support, the survival space of startups is extremely compressed. When evaluating investment projects, venture capital often avoids those tracks "hunted" by giant data, leading to the exhaustion of disruptive innovation at the source [8].

This phenomenon is not alarmist talk but a reality that has already emerged in multiple sub-sectors: startups either choose to be acquired by giants or perish in data scarcity. Meanwhile, in the absence of external competitive pressure, the innovation motivation of monopoly platforms themselves will also show marginal diminishing returns, tending to maintain the status quo through reparative innovation rather than engaging in potentially self-revolutionary disruptive innovation. Constructing a mandatory sharing system is essentially aimed at breaking this dual suppression. By introducing external competition to force giants to maintain the keenness of technological iteration, and simultaneously providing innovative "data fuel" for SMEs, it achieves the maximization of societal innovation welfare and the sustainable development of the digital economy.

3. LOCALIZED RECONSTRUCTION OF THE ESSENTIAL FACILITIES DOCTRINE: FROM PHYSICAL BOTTLENECKS TO DIGITAL GATEWAYS

As a classic tool in antitrust law for addressing the refusal to deal in natural monopoly industries, the Essential Facilities Doctrine (EFD) is premised on the principle that when a facility is indispensable for market competition and cannot be reasonably duplicated by competitors, the refusal of the facility controller to grant access constitutes monopolistic conduct. Originating in physical infrastructure sectors such as railways, ports, and power grids, the doctrine's jurisprudential foundation lies in balancing private property rights with the public interest to prevent the abuse of the natural monopoly attributes of infrastructure as tools for excluding competition. However, transplanting this doctrine-rooted in the industrial age-directly into the digital economy faces significant challenges of "acclimatization." The non-rivalrous nature of data means it is not limited by physical capacity, and simultaneous use by multiple parties does not deplete the value of the data itself. Meanwhile, the responsibilities of privacy protection, trade secret attributes, and cybersecurity risks carried by data constitute new obstacles to sharing that physical facilities do not possess. Therefore, it is necessary to undertake a dual reconstruction of "data-fication" and "localization" of the doctrine, combining the spirit of the amendment to China's Anti-Monopoly Law with the institutional supply of the "Data Twenty Measures."

3.1. The Justification for Theoretical Application: From Physical Facilities to Digital Infrastructure

Although the EFD has tended towards conservatism in Western judicial practice, as represented by the U.S. case Verizon v. Trinko [9], and has been criticized by some liberal scholars as "forced contracting that suppresses investment," the doctrine possesses a realistic soil for revival and jurisprudential legitimacy within the governance context of China's digital market.

Its primary premise lies in a profound recognition of the economic essence of the "infrastructuralization" of data elements. In the digital economy era, data is no longer merely a private competitive asset of enterprises but has evolved into a social foundational resource akin to water, electricity, and gas [10].Through long-term "two-sided market" operations, dominant platforms have accumulated basic data covering multiple dimensions such as user identity, social relationships, transaction credit, and behavioral preferences. These data substantially constitute "antecedent inputs" for downstream operators to enter the market and conduct business. Similar to physical infrastructure, this data accumulation features extremely high fixed costs and extremely low marginal replication costs, exhibiting significant natural monopoly characteristics. When a single platform controls over 90% of the underlying data in a specific field (such as instant messaging or online retail), it effectively masters the "Digital Gateway" to the digital market. At this point, the net loss of social welfare caused by the data controller's refusal of access-including the stagnation of downstream innovation, the loss of consumer choice, and the reduction of market efficiency-far outweighs the potential negative impact that mandatory sharing might have on upstream investment incentives. In the game between "efficiency" and "fairness," the systemic dividends brought by breaking "Digital Gateways" provide a solid efficiency defense for antitrust intervention.

Furthermore, the legislative purpose of *China's Anti-Monopoly Law focuses* not only on economic efficiency but also explicitly emphasizes "protecting fair market competition" and "safeguarding consumer interests and the public interest." This multi-value objective dictates that when dealing with data monopolies, one cannot simply copy the analytical framework of U.S. antitrust law based purely on "price theory," but should pay more attention to the openness and inclusiveness of the market structure. Therefore, identifying critical data with infrastructural attributes as "essential facilities" is an inevitable logic for antitrust law to adapt to the evolution of the digital economy form.

3.2. Institutional Resolution of Rights Conflicts: Allocation of Access Rights under Property Rights Separation

For a long time, the greatest jurisprudential obstacle hindering the application of the EFD in the data field has been the tension between the "absoluteness of private property rights" and the "public nature of mandatory sharing." Traditional views hold that mandating enterprises to open data they have invested heavily in collecting and organizing is tantamount to the expropriation of private property, which may fundamentally shake the property rights foundation of the market economy. However, the data property rights system reform promoted by China provides a highly innovative institutional supply to resolve this paradox.

The Opinions of the CPC Central Committee and the State Council on Building Basic Systems for Data to Better Play the Role of Data Elements (the "Data Twenty Measures") creatively proposes a "Tripartite Separation of Rights" framework: the right to hold data resources, the right to process and use data, and the right to operate data products [11]. The core of this institutional design lies in diluting the concept of "ownership" of data and shifting the emphasis to "holding" and "use." Under this framework, the application of the EFD no longer implies stripping data controllers of their "ownership" or requiring them to transfer the original copy of data assets, but rather focuses on restricted opening at the level of the "right to process and use."

Specifically, the legal consequence of mandatory data sharing is the establishment of a "non-exclusive access license." Through mandatory sharing, competitors obtain the right to develop and utilize the value of the data, rather than exclusive control over the data itself. Data controllers still retain the right to hold the original data and the right to operate derivative products developed based on that data. This "Allocation of Access Rights" model ingeniously transforms "expropriation of property" into "imposition of burdens" in jurisprudence-that is, while acknowledging the legitimate holding of data by platform enterprises, it imposes certain social obligations on them under antitrust law. This aligns with the modern rule-of-law concept that "property rights should serve the public welfare," while maximally preserving the core rights and interests of data controllers, achieving an incentive-compatible institutional balance.

3.3. Dynamic Reshaping of Constitutive Elements: Identification Standards Adapted to the Digital Ecosystem

After resolving the justification for theoretical application and rights conflicts, it is necessary to rigorously reconstruct the identification standards for "Essential Data." Traditional EFD requires facilities to be "physically impossible to duplicate," but in the digital world, data appears to be non-rivalrous and infinitely replicable, rendering traditional standards ineffective. Therefore, a "three-dimensional identification standard" adapted to the characteristics of the digital ecosystem must be established.

First, "Relative Non-substitutability" in the Ecological Dimension. In the digital economy, judging whether data is substitutable cannot rely solely on whether it can be technically re-collected, but should focus on "commercial feasibility" and "time barriers." If reconstructing a dataset of equivalent scale and dimension requires sunk costs exceeding reasonable commercial expectations, and due to the existence of network effects, new entrants cannot accumulate a user scale and data depth sufficient to compete with incumbents within a reasonable time, the data should be deemed to possess non-substitutability in the "ecological" sense. For example, although it is technically possible to develop a new social networking app, if the complex user relationship graph and historical interaction data accumulated by the dominant platform over a decade cannot be replicated, the new app cannot actually provide homogeneous competitive services, and thus the relationship graph constitutes a de facto essential facility.

Second, Public Necessity with "Systemic Importance." Not all high-value data are essential facilities. The objects of mandatory sharing should be strictly limited to data that acts as a "bottleneck" for downstream market competition, industry innovation, or the public interest. This element requires a strict causal test: public necessity is met only when the absence of specific data would lead to a widespread "service vacuum" in the downstream market, block key innovation paths, or result in a significant decline in consumer welfare. For instance, in the field of autonomous driving, if extreme road condition data controlled by a single enterprise becomes the sole bottleneck for the entire industry to improve algorithmic safety, and failure to share it would endanger public traffic safety, such data possesses public necessity. This limitation aims to prevent antitrust remedies from being abused as tools for competitors to steal core trade secrets, ensuring the modesty of institutional application.

Third, Technical Accessibility based on "Interoperability." Distinct from the physical opening of facilities, the sharing of data facilities must be based on technical feasibility. Another key prerequisite for identifying essential data is that, under existing technical conditions, secure data circulation and controlled use can be achieved through means such as Application Programming Interfaces (APIs), Privacy-Preserving Computation, or Federated Learning. This standard requires that when antitrust enforcement orders mandatory sharing, it must simultaneously consider compliance baselines with the Data Security Law and the Personal Information Protection Law. If mandatory sharing cannot technically resolve data desensitization issues, or if sharing would lead to systemic security risks (such as large-scale leakage of user privacy), then even if the data is ecologically non-substitutable, the EFD should not apply, and alternative legal remedies should be sought. Through the dynamic reshaping of these three standards, we can construct a framework for mandatory data sharing analysis that fits both digital technological characteristics and the reality of China's industrial development.

4. DATA CLASSIFICATION AND TRADE SECRET EXEMPTION MECHANISM FROM THE PERSPECTIVE OF RIGHTS BALANCE

After establishing the applicability of the Essential Facilities Doctrine in the digital economy, the focus of institutional construction shifts to precisely delineating the boundaries of mandatory sharing. Mandatory data sharing does not aim to eliminate the private attributes of data, nor is it an indiscriminate deprivation of enterprises' competitive advantages. Instead, it seeks a dynamic balance between promoting competition under antitrust law and protecting trade secrets under anti-unfair competition law. The realization of this balance relies on a classification and grading mechanism based on data value sources and competitive attributes. We need to discard the traditional ownership classification based on "personal information" or "public data" and instead, guided by the jurisprudential spirit of the separation of data holding rights and processing/use rights in the "Data Twenty Measures," construct a dual classification system centered on "Basic Operational Data" and "Derivative Value-Added Data." Based on this, we can establish differentiated sharing rules and trade secret exemption paths.

4.1. Basic Operational Data: Jurisprudential Logic of Principle Sharing and Interoperability Basic Operational Data

refers to data sets that are naturally generated, objectively recorded, and non-exclusive during the process of platform enterprises providing core services. Such data typically includes basic commodity information (SKUs) on e-commerce platforms, geographic coordinates of logistics and distribution, basic user node relationships on social networks, and interoperability protocols for instant messaging. From the perspective of the economic attributes of its generation mechanism, basic operational data is often a "by-product" of the platform's commercial activities rather than a "core product" developed through specialized intellectual resource investment [12]. For example, user clickstreams or transaction records on e-commerce platforms are primarily digital mappings of users' own behaviors.

Although the platform provides the venue and tools for recording, it has not performed creative intellectual processing on this raw data. Therefore, such data is closer to "factual information" than "intellectual property," and there lacks a solid jurisprudential basis for enjoying absolute exclusive control over it [13].

In the view of antitrust law, basic operational data often constitutes the boundary of the "relevant market" for downstream operators entering the market. When a super-platform uses its first-mover advantage to blockade such data within a closed ecosystem, it is essentially using a "by-product" to construct an artificial barrier to entry, blocking the interoperability of the digital economy. According to the reconstruction logic of the EFD, if such data meets the ecological non-substitutability criterion, it should be included in the scope of mandatory sharing. Implementing interoperability through APIs aims to restore a fair starting point for market competition, returning competition to the quality of products, service efficiency, and algorithmic superiority itself, rather than monopolistic control over underlying resources. Furthermore, mandatory sharing of such data can generate significant positive externalities. For instance, connecting commodity information databases and review systems across different e-commerce platforms can reduce multi-platform operating costs for merchants, eliminate search costs for consumers, and thereby improve the circulation efficiency of the entire digital supply chain. Therefore, for basic operational data that does not involve core algorithms and has undergone desensitization, the law should establish a regulatory orientation of "sharing as the principle, exemption as the exception," treating it as "general infrastructure" of the digital society to be opened.

4.2. Derivative Value-Added Data: Principle Exemption and the Defensive Bottom Line of Innovation Incentives

In sharp contrast to basic operational data is Derivative Value-Added Data. This refers to data products with predictive, decision-making, or unique commercial value formed after enterprises invest significant capital, computing power, and intellectual resources to deeply cleanse, mine, and train models on raw data. Typical derivative value-added data includes credit risk scoring models of fintech companies, personalized recommendation algorithm parameters of content platforms, road condition decision trees of autonomous driving systems, and market trend prediction reports derived from complex calculations. From a jurisprudential perspective, such data has completely detached from the category of raw information, deeply condensing the unique competitive advantages and intellectual labor of the data controller. It possesses significant property attributes and intellectual property characteristics, often falling under the protection of core trade secrets.

For derivative value-added data, the mandatory sharing system must maintain a high degree of modesty and prudence. If enterprises are indiscriminately required to open algorithm models or high-value analysis data in which they have invested heavily, it will directly induce severe "free-riding" behavior. Competitors will no longer have the motivation to engage in independent algorithmic innovation and data mining but will tend to wait and directly demand ready-made results from industry leaders. This "perverse incentive" (or disincentive) will lead to a contraction of R&D investment in the entire industry, causing enterprises to prefer locking data in a "black box" rather than engaging in deep development, ultimately damaging the long-term innovation vitality of the digital economy. Therefore, derivative value-added data should in principle be excluded from the scope of mandatory sharing, subject to the rule of "exemption as the principle, sharing as the exception."

Only in extremely rare and exceptional circumstances-where the data has become the sole resource concerning the national economy and people's livelihood (such as epidemic transmission models during public health crises or natural disaster warning data) and cannot be obtained through other channels-can a mandatory licensing procedure be initiated. Even in such exceptional cases, strict "necessity tests" and the principle of "least intrusion" must be followed, accompanied by high compensation mechanisms to ensure that the innovation returns of data controllers are not damaged

by sharing. This strict distinction is precisely to draw a clear line between the sword of antitrust law breaking blockades and the shield of anti-unfair competition law protecting innovation.

4.3. Trade Secret Defense: Substantive Review and Dynamic Allocation of Burden of Proof

In judicial and enforcement practice, data controllers often tend to generalize the concept of "trade secrets," labeling all undisclosed data (including basic operational data that should be shared) as trade secrets to evade mandatory sharing obligations. To prevent trade secrets from becoming a "safe harbor" for data monopolies, a rigorous defense review procedure and burden of proof allocation mechanism must be constructed.

First, a judicial review standard for "Substantive Secrets" should be established. When claiming trade secret exemption, data controllers cannot rely solely on the "undisclosed status" of data or internal confidentiality agreements for a formal defense. Instead, they must prove that the data meets the three statutory elements of "secrecy," "confidentiality," and "commercial value" as stipulated in the *Anti-Unfair Competition Law* [14]. More critically, the controller needs to prove that the disclosure of such data would directly lead to the loss of its core competitive advantage, rather than merely increasing the convenience for competitors. If the so-called "secret" is merely a collection of information that can be gathered through public channels, or data obtained through reverse engineering via conventional technical means, courts and enforcement agencies should not support the exemption request.

Second, regarding the allocation of the burden of proof, a mechanism of "Reversal of Burden of Proof" (or dynamic shifting) should be introduced. Considering that the data requester is usually in a disadvantaged position of information asymmetry and finds it difficult to judge the specific composition and technical details of data through external observation, once the requester preliminarily proves the "necessity," "non-substitutability," and the competitive harm caused by the refusal to open, the burden of proof shifts to the data controller. The controller must bear the responsibility of proving that its refusal has a "justifiable reason." Such justifiable reasons should be objective and concrete, for example, proving that sharing the data would lead to the leakage of its core algorithm source code, trigger systemic cybersecurity risks, or that it is impossible to desensitize the data without violating the *Personal Information Protection Law*.

Finally, to resolve the identification difficulties caused by the "Data Black Box," an independent third-party "Algorithmic Auditing" or "Data Trusteeship" mechanism should be introduced as an institutional buffer. When there is a fundamental disagreement between the two parties regarding the secret attributes and sharing risks of the data, the court or regulatory agency may entrust a credible third-party professional technical institution to intervene. In a "black box" environment, the third party conducts desensitization testing and security assessment on the data, or uses "Privacy-Preserving Computation" (data available but not visible) technology. This satisfies the requester's need for data value while ensuring that the controller's original code and core secrets are not directly exposed. This procedural design aims to compensate for the limitations of legal judgment through technical rationality, achieving a substantive resolution of rights conflicts within the framework of procedural justice.

5. IMPLEMENTATION PATH OF THE MANDATORY SHARING SYSTEM: PRICING, REGULATION, AND REMEDIES

Having completed the theoretical reconstruction and boundary delineation, the practical implementation of the mandatory data sharing system relies on a refined execution mechanism. This involves not only establishing a fair sharing consideration for intangible data assets but also constructing a normalized administrative regulation and judicial remedy system to ensure the system

is not hollowed out or alienated during operation [15]. We must be vigilant against "rights on paper" failing to translate into "competition in fact." Therefore, it is particularly urgent to construct a closed-loop implementation path covering pricing, regulation, and remedies.

5.1. Accounting Mechanism for Sharing Consideration: Differentiated Pricing based on FRAND Principles

Mandatory sharing does not imply "free-riding" or the expropriation of private property. To maintain the motivation of data controllers to continuously maintain infrastructure and to prevent excessive demands from data requesters, a pricing system based on "Fair, Reasonable, and Non-Discriminatory" (FRAND) principles must be established [16]. However, the intangible and non-rivalrous nature of data means its marginal cost approaches zero, rendering traditional pricing rules based on marginal cost ineffective. Therefore, a dual-track pricing model combining "Cost Plus Reasonable Profit" and "Value Orientation" is required.

For Basic Operational Data defined as quasi-public facilities, pricing should reference the regulatory logic of public utilities, adopting a low-price strategy oriented towards cost recovery. The lower limit of fees should cover the direct costs of data cleansing, desensitization, API development, and server bandwidth maintenance to ensure data controllers do not incur losses due to sharing obligations. The upper limit should be strictly regulated to prevent monopoly enterprises from unreasonably allocating sunk costs (such as early marketing expenses) to sharing fees, thereby disguising high licensing fees to obstruct competitor access.

For Derivative Data involving intellectual value-add or high-value data opened under exceptional circumstances, a value-oriented pricing strategy should apply, allowing data controllers to charge a reasonable premium reflecting their R&D investment, scarcity, and market supply and demand. Pricing here is not merely compensation for costs but a return on innovation. To prevent price discrimination, antitrust enforcement agencies should require dominant platforms to publish a "Standard Interoperability Rate Card," clarifying charging standards for different data dimensions, calling frequencies, and service levels. This ensures that all qualified downstream operators-regardless of market share or whether they compete with the platform-can obtain data on equal terms, eliminating the survival space for price discrimination at the source.

5.2. Dynamic Reshaping of Administrative Regulation: From "Ex Post Punishment" to "Penetrating Supervision"

Due to the highly concealed, real-time, and technically complex nature of data circulation, the traditional static antitrust enforcement mode of "ex post filing, investigation, and punishment" often fails to produce substantial deterrence. By the time an enforcement agency makes a penalty decision, the victimized startup may have already collapsed due to data cutoff. Therefore, the national antitrust enforcement agency should explore establishing a "Full-Cycle" Dynamic Regulatory Mechanism adapted to the characteristics of the digital economy [17].

The core of this regulatory reshaping is shifting from regulating behavioral outcomes to regulating technical architecture. Specifically, regulatory agencies should require super-platforms identified as "Gatekeepers" to establish a mandatory interoperability compliance system. This includes regular reporting on the opening of data interfaces, API call success rates, latency data, and detailed records of reasons for access refusal. To resolve information asymmetry between regulators and platforms, an independent third-party "Algorithmic Auditing" or "Data Trustee" system should be introduced. Professional technical teams appointed or recognized by regulatory departments shall have the authority to penetrate the platform's technical underpinnings. They will conduct "Penetrating Supervision" on interoperability protocols to screen for technical practices where platforms implement "disguised refusals" by intentionally reducing API response speeds, blurring data granularity, or frequently changing interface standards.

For verified malicious blocking behaviors, administrative enforcement measures should shift from single fines to "Behavioral Remedies." In addition to imposing high fines under the *Anti-Monopoly Law*, enforcement agencies should actively employ corrective measures such as ordering the opening of interfaces within a time limit, mandating the modification of interoperability protocols, and cancelling discriminatory restrictive clauses. In extreme cases involving recalcitrant monopolistic behaviors that severely hinder industry innovation despite repeated warnings, "Structural Remedies"-such as the mandatory divestiture of data business units-may be explored to completely sever the roots of data monopoly.

5.3. Perfection of the Judicial Remedy System: Synergy between Interim Injunctions and Punitive Damages

Beyond administrative regulation, judicial remedy is the last line of defense for safeguarding enterprise data rights. However, competition in the digital market changes rapidly, and a "winner-takes-all" landscape often forms within a short period. Traditional damage compensation litigation faces the dilemma of "delayed remedy" due to long cycles and difficulties in quantifying losses. Therefore, a judicial remedy system prioritizing Interim Injunctions (Behavior Preservation) backed by Punitive Damages must be constructed.

First, the threshold for applying Interim Injunctions (*Act Preservation in Chinese Civil Procedure*) in data disputes should be significantly lowered. When a data requester can preliminarily prove that the data is essential for its survival and that refusal to open will cause "irreparable harm" (such as irreversible loss of market share or loss of key business opportunities), courts should be bold in issuing temporary injunctions for mandatory access [18]. Establishing a judicial orientation of "Access First, Settle Later" ensures that competitors' businesses are not interrupted during lengthy litigation, maintaining market competitive vitality.

Second, for serious monopolistic behaviors involving malicious refusal to share, false opening, or violation of administrative orders, Punitive Damages should be actively applied. Given that losses caused by data monopolies are often concealed and diffuse (e.g., stifling potential innovation gains), using direct economic loss as the sole basis for compensation fails to provide sufficient deterrence. Courts may, in accordance with the *Anti-Monopoly Law* and relevant judicial interpretations, apply punitive damages of one to five times the calculated amount on the basis of infringement profits or losses suffered, significantly raising the cost of violating the law. Meanwhile, regarding the burden of proof for calculating damages, when the right holder has done their best to provide evidence but the exact amount remains undeterminable, courts should exercise discretion to determine a reasonable compensation amount based on the nature, duration, and consequences of the infringement, avoiding the judicial embarrassment of "low compensation due to calculation difficulties."

6. CONCLUSION

The wave of the digital economy is reshaping the global competitive landscape. As a core factor of production, the allocation efficiency of data directly bears on the long-term competitiveness of a nation's digital economy. The introduction and localized reconstruction of the Essential Facilities Doctrine provide a theoretical key to resolving the eternal tension between data monopoly and innovation incentives.

By defining essential data as the "New Infrastructure" of the digital economy and constructing a classified and hierarchical sharing mechanism based on Basic Operational Data and Derivative Value-Added Data, we attempt to chart a "Chinese Path" that transcends traditional European and American approaches. This institutional scheme acknowledges the legitimate rights and interests of dominant platforms in data assets, avoiding rude interventions akin to "expropriation"; at the same time, through mandatory interoperability requirements, it breaks the blockade of "Walled Gardens"

on market vitality, ensuring that SMEs and innovators can fairly access the survival guarantees of the digital age.

Of course, the vitality of any system lies in its implementation. The establishment of a mandatory data sharing system is not a once-and-for-all solution; it requires continuous tuning and friction among antitrust enforcement agencies, the judiciary, and industry players in practice. As algorithmic technologies iterate and business models evolve, the connotation of essential data, the boundaries of sharing, and the technical means of regulation must also advance with the times. Yet, regardless of how forms change, the core objective remains constant: to ensure, through structural legal adjustments, that data-this critical element-flows in the sunlight, allowing the dividends of the digital economy to benefit every market entity and consumer.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGEMENTS

Funding:Supported by the Outstanding Innovative Talents Cultivation Funded Programs for Doctoral Students of Jinan University (2024CXB005).

REFERENCES

[1] CPC Central Committee and State Council, “Opinions on Building Basic Systems for Data to Better Play the Role of Data Elements”, Dec. 19, 2022.

[2] Lina M. Khan, “Amazon’s Antitrust Paradox”, Yale Law Journal, vol. 126, 2017, pp. 710-805.

[3] Robert Pitofsky et al., “The Essential Facilities Doctrine Under U.S. Antitrust Law”, Antitrust Law Journal, vol. 70, no. 2, 2002, pp. 443-462.

[4] Merton, R. K. (1968). The Matthew effect in science: The reward and communication systems of science are considered. Science, 159(3810), 56-63.

[5] Daniel L. Rubinfeld and Michal S. Gal, “Access Barriers to Big Data”, Arizona Law Review, vol. 59, 2017, pp. 339-381.

[6] Sidak, G. and Teece, D. (2009) Dynamic Competition in Antitrust Law. Journal of Competition Law & Economics, 5(4), 581-631.

[7] Stigler Committee on Digital Platforms, Final Report, Stigler Center for the Study of the Economy and the State, 2019, p. 102.

[8] Schumpeter, J. (1942). Capitalism, Socialism and Democracy. New York: Harper and Brothers.

[9] Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004).

[10] Viktor Mayer-Schönberger and Thomas Ramge, Reinventing Capitalism in the Age of Big Data, Basic Books, 2018, p. 150.

[11] CPC Central Committee and State Council, “Opinions on Building Basic Systems for Data to Better Play the Role of Data Elements”, Dec. 19, 2022.

[12] Inge Graef, EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility, Kluwer Law International, 2016.

[13] Wolfgang Kerber, “Rights on Data: The EU Perspective”, in Data as Counter-Performance – Contract Law 2.0?, Springer, 2017.

[14] Standing Committee of the National People's Congress, Anti-Unfair Competition Law of the People's Republic of China, Article 9, revised April 23, 2019.

[15] Jin Sun, “Antitrust Regulation of Digital Platforms”, Social Sciences in China, no. 5, 2021, pp. 101-127.

[16] Anne Layne-Farrar et al., “Pricing Patents for Licensing in Standard-Setting Organizations”, Antitrust Law Journal, vol. 74, 2007, pp. 671-706.

[17] Herbert Hovenkamp, “Antitrust and Platform Monopoly”, Yale Law Journal, vol. 130, 2021, pp. 1901-1974.

[18] Gregory Sidak and David Teece, “Dynamic Competition in Antitrust Law”, Journal of Competition Law & Economics, vol. 5, no. 4, 2009, pp. 581-631.