Philosophy and Social Science Vol. 2 No. 10, 2025

Under the Perspective of Anti-monopoly: Expansion of Digital Platform Gatekeeper Obligation and Responsibility Shaping

Zexiu Li
Xiangtan University, Xiangtan, Hunan, China

Abstract: Given the super-network effects of data, algorithms, and interfaces that enable leading digital platforms to assume the triple identity of "market player-rule-maker-de facto regulator," traditional antitrust tools centered on price analysis and ex post remedies have fallen into systemic failure. Comparative studies of U.S. ex post enforcement, the EU's Digital Markets Act, Germany's GWB10, and the UK's DMCC practices reveal that the "gatekeeper" paradigm is replacing pure dominance regulation as a key approach to addressing platform competition disorder and governance vacuum. Accordingly, a ternary framework of gatekeeper responsibilities applicable to China can be constructed. First, in the dimension of competitive order, a negative list should be implemented alongside mandatory disclosure for small acquisitions, while institutionalizing data portability and interface interoperability obligations to weaken lock-in effects. Second, in the dimension of public governance, third-party algorithmic transparency audits, entrusted data sharing pools, and public interface standards should be introduced to encourage platforms to internalize algorithmic biases and information risks. Third, in the dimension of pluralistic values, differentiated encryption, compliance sandboxes, and proportionate enforcement tools can be employed to achieve a dynamic balance between efficiency, innovation, and fairness. This framework aims to address the externalities posed by the infrastructure of platforms, providing an operational institutional blueprint for digital economy governance, demonstrating that expanding gatekeeper obligations is a dual path to preventing monopolies and activating sustainable innovation.

Keywords: Digital Platform; Gatekeeper; Anti-Monopoly; Data Portability; Platform Economy

1. Structural Challenges of Digital Economy and Paradigm Change of Antitrust Regulation

The digital economy, propelled by platform models, has unleashed unprecedented innovative energy and economic vitality. However, the root of this vitality lies deeply embedded in a unique logic of power accumulation, [1] fundamentally challenging the theoretical foundations and institutional frameworks of traditional antitrust law. [2] The rise of digital platforms is not merely an expansion of market power, but a qualitative transformation of market structure and competition paradigms. This transformation renders existing regulatory tools inadequate, making a systematic examination of the mechanisms behind platform power generation and the failure of traditional analytical frameworks the logical starting point for exploring paradigm shifts.

1.1 The Generation Logic of Platform Power and the Failure of the Traditional Anti-monopoly Analysis Framework

Over the past decade, China's digital economy has experienced exponential growth, with transaction-matching platforms, content-sharing platforms, and ecosystem-operated internet platforms springing up like mushrooms after rain. These platforms leverage data, algorithmic models, and cross-scenario interfaces [3] to create a reinforced network effect catalyzed by "economies of scale, economies of scope, and data advantages [4]." This has not only shaped a new paradigm for value creation but also given rise to structural challenges that disrupt traditional regulatory frameworks.

First, platforms simultaneously connect multilateral users. The direct network effect of "the more you use, the more value you get" and the indirect network effect of "the more users, the more data; the more data, the higher barriers" reinforce each other, creating a market landscape

of "winner-takes-all" dominance, closed ecosystems, and even "ecosystem encirclement." By leveraging this, super-large platforms control the three critical levers of "entry points, protocols, and standards," granting them the power to dictate whether and how information, goods, and capital pass through these gateways-a capability that transcends the scope of traditional operators.

Second, in zero-price or multilateral market scenarios, the "price-output" metric fails to accurately reflect welfare changes. The multipurpose nature of data and the diversity of business ecosystems lead to a "dynamic drift" in market definition. Moreover, case-by-case and ex post enforcement often suffers from procedural red tape and information asymmetry, allowing practices like predatory acquisitions, self-preferential treatment, and discriminatory ranking to become entrenched as "established facts" before regulatory implementation.

Third, at the technological level, risks such as algorithmic black boxes, privacy erosion, and information cocoons continue to accumulate. Economically, vertical integration and vertical bundling are eroding the survival space for innovative small and medium-sized enterprises. Socially, platforms are increasingly shaping public discourse and cultural diversity. The interplay of "platform-user-society" triple externalities creates systemic risk, necessitating a regulatory shift from case-by-case remediation to structural prevention.

1.2 The Genealogy and Evolution of the "Gatekeeper" Theory and the Application Dilemma of Localization

To address the inherent shortcomings of traditional competition law-characterized by delayed responses and inadequate intervention in digital markets-the global regulatory paradigm is undergoing a profound transformation. The European Union has spearheaded this shift, with its Digital Markets Act (DMA) taking effect in late 2022 and gradually coming into force from 2023. The Act seeks to reshape market competition by identifying "gatekeeper" platforms and imposing a suite of ex-ante obligations, including ensuring data portability, enabling key service interoperability, complying with a "negative list" of prohibited practices, and strengthening merger reporting requirements.

Beyond the European Union, major economies have adopted diverse approaches to address digital market competition. Some nations have pioneered localized preemptive regulatory frameworks. Germany, for instance, introduced Article 19a through its 2021 tenth amendment to the German Competition Act [5] (GWB Digitalisation Act), granting regulators the authority to designate companies with "supreme cross-market importance" and impose pre-emptive obligations. The UK formally enacted the Digital Markets, Competition and Consumers Act (DMCC) in 2024, empowering its Digital Markets Department to identify enterprises with "strategic market position" and enforce customized conduct rules. In contrast, while the U.S. Congress has reviewed multiple "platform antitrust" proposals, no unified federal legislation has been established, leaving regulatory focus on judicial interpretation of existing antitrust laws. Other countries have pursued more varied approaches: Australia is developing a flexible regulatory system for mandatory conduct rules, while Canada prioritizes modernizing its Competition Act to address digital economy challenges. These differentiated institutional choices collectively form a complex global landscape of regulatory convergence and localization, centered on the "gatekeeper" concept to strengthen platform accountability.

The concept of "gatekeepers" originated from communication studies' focus on the "gate effect" of information flow. At its core, it highlights the inherent multi-sided matchmaking function of digital platforms, which inherently endows them with gatekeeping attributes. By controlling interfaces and standards, these platforms can determine whether commercial and end users can "enter the gate," thereby shaping competitive landscapes and social resource allocation. Notably, the gatekeeper theory has undergone two paradigm shifts in legal practice: traditional gatekeepers-serving as auxiliary state regulators with third-party oversight duties [6] (e.g., auditors, lawyers); and modern gatekeepers-super platforms as regulated entities that assume dual roles of passive competition obligations and active public obligations.

However, the localization of this theory faces significant systemic challenges in China. The academic and legislative practices in our country have yet to form a clear typological distinction between the two types of gatekeepers mentioned above, leading to a situation where multiple

policy tools exhibit "terminological convergence and logical fragmentation" in their regulatory objectives. For example, although Article 58 of the Personal Information Protection Law imposes additional obligations on "large platforms," its focus lies in data governance rather than market competition structure. The State Administration for Market Regulation once issued the "Guidelines for Classification and Grading of Internet Platforms (Draft for Comments)" to identify "ultra-large platforms," but the guidelines have not been officially implemented after several years, reflecting the prudence and balance of the regulatory authorities in setting standards.

The deeper reason lies in the fact that a consensus has yet to be formed in China regarding the core controversy of platform regulation. The two major questions-whether there exists a "structural failure" in China's digital market that [7] urgently requires preemptive intervention, and whether the "gatekeeper" system will "stifle innovation" rather than "foster competition" -continuously influence the ultimate direction of policy. Especially in recent years, against the macro background of regulatory tone shifting to emphasize "routine regulation" and "promoting healthy development," the path of fully introducing a "gatekeeper"-style strong regulatory framework has become increasingly cautious. Regulatory practices tend to make case-by-case, precise adjustments within the existing legal framework, causing the localized construction of the "gatekeeper" system to advance slowly amidst theoretical debates and practical explorations.

2. Externally: The Institutional Practice of the Duty of Digital Platform Gatekeeper

The evolution of digital platform gatekeepers' obligations has been a gradual process, reflecting a profound paradigm shift in regulatory approaches-from "post-facto sanctions" to "preemptive prevention" and ultimately "structural adjustments." This paradigm shift represents not merely an addition to legal tools, but a fundamental revolution in market power dynamics, competitive principles, and regulatory philosophy. It signifies a transition from passive responses to existing damages to proactive shaping of market structures, and a shift in enforcement focus from complex case-by-case causality analysis to establishing clear behavioral standards for market entities. The institutional practices of major global economies provide rich examples for observing this transformation.

2.1 Practice and Limitation of the American Traditional Antitrust Law Enforcement

While the United States has not explicitly adopted the term "gatekeeper" in regulating digital platforms, its early antitrust enforcement practices had already addressed the competitive risks posed by platforms as gateways. As early as the late 20th century, the U.S. Department of Justice applied the traditional framework of the Sherman Antitrust Act in a lawsuit against Microsoft for bundling browser sales and abusing its dominant operating system position. By defining relevant markets, identifying dominant positions, and penalizing abusive practices, the Justice Department safeguarded market competition-a pioneering judicial approach that laid the groundwork for addressing tech giants.

However, as the 21st century dawned and new-generation platforms emerged, the limitations of this traditional "post-facto" enforcement model became increasingly apparent. First, regulatory practices in merger review demonstrated notable leniency. The most controversial and far-reaching cases involved the Federal Trade Commission (FTC) approving landmark acquisitions: Google's 2007 acquisition of DoubleClick, Meta's 2012 purchase of Instagram, and WhatsApp's 2014 takeover. Despite early warnings about how these mergers would stifle competition through data consolidation and create insurmountable market barriers, regulators failed to fully anticipate their long-term competitive damage under conventional frameworks. [8] These cases, now widely regarded as "enforcement failures," starkly exposed the shortcomings of post-facto review mechanisms in addressing "killer acquisitions" and evaluating data-driven advantages.

Secondly, in judicial practice, courts 'interpretation of the platform economy model has constrained enforcement effectiveness. In the landmark case Ohio v. American Express Co., the Supreme Court's "bilateral market" framework required evaluating both ends of the platform's impact on users whenassessing anticompetitive effects, significantly increasing the government's burden of proof. [9] This

precedent has made challenging platforms' common "anti-steering provisions" and similar practices exceptionally difficult, revealing the limitations of traditional judicial doctrine in adapting to the complex business models of digital platforms.

These challenges in law enforcement and judicial systems have jointly given rise to critical ideologies represented by "New Brandesianism," driving profound transformations in U.S. regulatory philosophy in recent years. The landmark antitrust lawsuits filed by the Department of Justice and the Federal Trade Commission against Amazon in 2023 and Apple in 2024 mark a strategic shift in enforcement priorities-from focusing on consumer prices to addressing structural suppression of competition, innovation, and workers by digital platforms. While Congress ultimately failed to pass legislation like the American Innovation and Choice Online Act aimed at establishing preemptive regulations, these far-reaching legislative efforts, combined with current aggressive enforcement, create a "dual-track" regulatory dynamic. This indicates that U.S. platform regulation is transitioning from traditional laissez-faire policies to more proactive interventions. The underlying logic aligns with the EU's "gatekeeper" system in core objectives like curbing self-preferential treatment and breaking ecosystem lock-in, achieving "different paths leading to the same destination."[10]

2.2 Systematic Construction of EU Digital Market Law

The EU's regulation of digital platform gatekeepers is rooted in its profound insight into the "failure" of traditional antitrust laws in the digital economy. Although the European Commission has imposed billions of euros in fines on Google for abusing its search market dominance and bundling Android systems, these post-fine sanctions failed to fundamentally alter its structural dominance. Instead, they exposed the limitations of traditional competition law-its "case-by-case analysis, time-consuming process, and delayed effects." In light of this and strategic considerations for domestic digital industry competitiveness and digital sovereignty, the EU proactively sought an institutional tool capable of proactively shaping market structures and ensuring fair competition. TheDigital Markets Act emerged as a result, with its legislative intent clearly targeting platforms that connect massive user bases and exert decisive influence on markets, granting them a special legal status as "gatekeepers."[11]

The Digital Markets Act (DMA), fully implemented since May 2023, establishes clear pre-approval obligations for designated "gatekeeper" platforms. [12] The identification criteria are systematically structured: First, the regulation targets ten core platform services (including online intermediaries, search engines, operating systems, and online advertising services). Second, the determination combines qualitative and quantitative standards. Qualitative criteria include significant influence on the EU internal market, serving as a key intermediary channel between business users and end-users, and maintaining a stable and enduring market position. Quantitative criteria encompass financial indicators (annual turnover in the EU of ≥7.5 billion euros or market capitalization of ≥75 billion euros over the past three years) and user metrics (monthly active end-users in the EU of ≥45 million and annual active business users of ≥10,000 in the past year). For platforms that partially meet quantitative standards but satisfy qualitative conditions, the European Commission may conduct flexible assessments through market research, considering factors such as network effects, data-driven advantages, user lock-in, and vertical integration.[13]

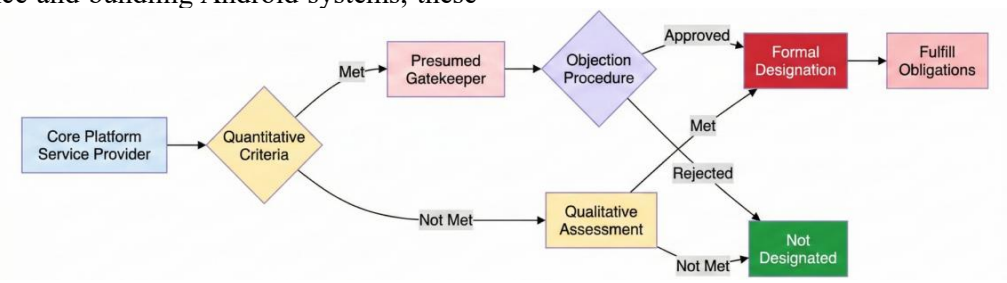

Figure 1. EU DMA Gatekeeper Identification Flowchart

Once designated as a "gatekeeper," the platform must comply with obligations outlined in the "blacklist" and "gray list." Article 5 of the Data Management Act (DMA) explicitly prohibits

self-preferential treatment and bundled services, aiming to eliminate business practices that have been repeatedly proven harmful. Article 6 outlines proactive obligations for platforms, including allowing users to uninstall pre-installed software, ensuring access to third-party app stores, and providing data portability, while allowing flexibility for compliant design. Additionally, Article 7 imposes highly anticipated interoperability requirements for major instant messaging services, seeking to break down closed communication ecosystems.

More importantly, the Digital Markets Act (DMA) has transitioned from legal text to complex enforcement practices and industrial competition. In September 2023, the European Commission designated Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft as the first gatekeepers. Since the March 2024 compliance deadline, while platforms have rolled out adjustment plans, the Commission has swiftly initiated non-compliance investigations into Alphabet's search ranking algorithm, Apple's App Store rules, and Meta's "pay or consent" model. These swift enforcement actions mark the formal entry of digital platform regulation into a "preemptive prevention" era characterized by proactive shaping and continuous oversight. The approach aims to fundamentally ensure fairness and competitiveness in digital markets through predefined behavioral boundaries and mandatory open interfaces.[14]

2.3 Evolution within the Paradigm: Legal Internalization in Germany and Empowerment Regulation in Britain

After the EU DMA established the paradigm of pre-regulation, Germany and Britain, as the major economies in Europe, responded quickly, but their institutional paths were not simply copied, but showed the differentiated evolution based on their own legal tradition and regulatory philosophy.

2.3.1 Legal internalization in germany: Strengthening regulation within the existing framework

Germany has integrated its "gatekeeper" philosophy into its existing antitrust framework. The landmark Article 19a of the German Competition Act (GWB), enacted in January 2021, authorizes the Federal Cartel Office (FCO) to designate companies with "paramount significance for competition across markets" as special regulatory targets. These entities face direct prohibitions on practices like preferential treatment and restricted data usage. [15] Since its implementation, the FCO has applied Article 19a to major tech giants including Google, Meta, Amazon, and Apple, demonstrating its commitment to embedding ex ante regulations into routine antitrust enforcement.

2.3.2 Empowerment regulation in the UK: Establishing professional institutions and customized rules

The UK has adopted a distinct approach through its "empowerment-based regulation" model. The Digital Markets, Competition and Consumers Act 2024 (DMCC), which came into force in 2025, authorizes the newly established Digital Markets Unit (DMU) to designate companies with "Strategic Market Status" (SMS). The UK's model is unique in that it does not impose a uniform "list of obligations," but instead requires the DMU to develop legally binding "code of conduct" for each designated SMS company. These codes will focus on three statutory objectives-fair trade, open choice, and trust and transparency-to precisely address core competition issues on specific platforms.

In contrast, Germany has upgraded its traditional antitrust legal arsenal, while the UK has developed a new, more flexible "professional toolkit". The German model is more efficient and predictable, though potentially less targeted. The UK model, however, is precise and adaptable to diverse platform business models, but demands exceptional expertise and resources from regulators. The coexistence of these two approaches offers a rich array of practical examples for global digital platform regulation, spanning from "pre-emptive legislation" to "pre-emptive supervision".

3. The Driving Logic and Normative Guidance of Goalkeeper Obligation Expansion

A paradigm shift in regulation centered on "preemptive prevention" has taken global shape, and this profound institutional transformation is no accident. Underlying this movement lies a progressive logic that compels legislative and enforcement bodies to transcend traditional frameworks, imposing broader and more interventionist obligations on gatekeepers. This logic can be deconstructed into three core dimensions: market-level competition disorder, societal demands for public governance, and

value-level rebalancing of multiple objectives. The profound insight into structural competition disorder in digital markets serves as the most direct and fundamental catalyst for this transformation, thus becoming the logical starting point for analysis.

3.1 Competition Disorder Driving: From Post-Sanction to Structural Prevention

The digital platform with its unique business model and technological advantages presents a "winner takes all" situation in the market competition, which makes the self-repair mechanism of the market fail in a specific field.

3.1.1 Super network effect and structural locking of data monopoly

The core competitiveness of digital platforms stems from their powerful network effects. Acting as intermediaries in multilateral markets, their value grows exponentially with user scale-where direct network effects like 'the more you use, the more valuable it becomes' and indirect network effects like 'data-algorithm-barriers' reinforce each other, forming a positive feedback loop. This enables leading platforms to rapidly reach market tipping points and establish structural barriers that new entrants find hard to overcome.

Data has become the decisive factor for businesses to succeed in the digital economy era. Major digital platforms leverage their monopolistic control over massive data to create precise user profiles, optimize algorithms, and deliver personalized recommendations. This allows them to extend their dominance from core sectors to adjacent markets, forming "dual monopoly" or "ecosystem monopolies." They further strengthen user lock-in effects-making it costly for consumers or business users to switch platforms, thus compelling them to remain loyal. Statistics reveal that European users spend disproportionately high time on Google and Facebook, with one-third of Germans relying solely on Booking for hotel bookings, demonstrating platforms' strong user retention and high switching costs. In the absence of effective competition, platforms no longer guarantee optimal services, forcing business users to accept unequal terms due to path dependence. Traditional antitrust frameworks centered on pricing prove inadequate when addressing structural issues in zero-price or multi-sided markets.[16]

3.1.2 Typical failure scenarios: From killer acquisition to ecosystem lockdown

The dynamic nature of the digital economy has given rise to various competitive failure scenarios that traditional antitrust tools struggle to effectively address.

First, the Killer Acquisition strategy. Major platforms eliminate potential competitors through mergers and acquisitions before they can pose a threat. Meta's strategic acquisitions of Instagram and WhatsApp exemplify this approach, aiming to consolidate its dominance in the social media sector. Since acquired companies often fail to meet the regulatory thresholds for traditional M&A reviews, competitive innovation ecosystems face severe suppression. [17] This is precisely the core issue addressed by the EU's Data Protection Regulation (DPR) that strengthens disclosure requirements, as well as the calls from national competition authorities for reforming review mechanisms.

Second, discriminatory practices and self-preferencing. Gatekeeper platforms controlling traffic entry points manipulate search rankings, feed recommendations, and product display priorities through algorithms to prioritize their own products/services or discriminate against other platform operators. Examples include e-commerce platforms forcing merchants into "either-or" choices and large platforms exploiting merchants' private data to develop competing businesses. Traditional antitrust laws, with their post-facto analysis and lengthy litigation processes, make it difficult to intervene effectively before or during the initial stages of harm.

Third, the refusal to trade critical resources and ecological blockade. Platforms leverage their monopolistic control over core data, technical interfaces, and operating systems to deny competitors access to "Essential Facilities." For instance, Apple has long restricted third-party payment services from using its NFC interface to maintain the exclusivity of Apple Pay. Such practices have been a key focus of the European Commission's antitrust investigation into Apple and the U.S. Department of Justice's 2024 antitrust lawsuit against the company. These measures essentially create data barriers and platform ecosystem barriers, hindering the growth of new market entrants and smaller competitors.

The above scenario shows that the large platform is not only a market participant, but also a

"market shaper" in fact by virtue of technology and rules. If the "quasi-regulatory" power is not effectively constrained, it will continue to aggravate market distortion, which constitutes the most fundamental motivation for the expansion of gatekeeper obligation.[18]

3.2 Public Governance Driven: Infrastructure of Platform and Internalization of Externality

The deep integration of digital platforms into socio-economic systems has transformed their role beyond mere commercial entities, increasingly assuming the quasi-public nature of critical infrastructure. This paradigm shift introduces new risks that traditional governance models cannot adequately address. To tackle these challenges, it is imperative to expand gatekeeper obligations, compelling platforms to internalize the social costs they previously externalized as part of their governance responsibilities.

3.2.1 Algorithmic black box: The emergence and externalization of systemic risk

As the "heart" powering digital platforms, algorithms create a "black box" that is difficult for outsiders to comprehend, predict, or effectively regulate. Their inherent power opacity and information asymmetry give rise to multi-layered systemic information risks. [19] When these risks materialize, the costs are often not borne by the platforms themselves but are instead shifted onto users and even society as a whole, representing a classic case of negative externalities.

The "black box nature" of algorithms first manifests as erosion of social equity. Embedded or amplified structural biases during algorithm design and training, combined with the broad data sources and nonlinear training processes, render these inherent biases difficult to detect and explain. In areas like credit approval, recruitment recommendations, ad targeting, and content moderation, algorithmic outputs often result in unfair treatment of specific groups (based on gender, age, region, occupation, etc.), creating what are termed "allocative harm" and "representational harm." As algorithms mass-produce and automate such biases, their impact rapidly expands. Given the complexity and opacity of algorithmic decision-making, victims struggle to identify the root causes of discrimination, let alone provide effective evidence or trace the origins. This creates an "excuse culture" for discriminatory outcomes, posing profound challenges to the principles of social equity.

Furthermore, the algorithm's "cognitive externality" undermines public discourse. While personalized recommendations enhance user experience, they create "information cocoons" that exacerbate social fragmentation, undermining the foundation of social consensus. Through implicit mechanisms like traffic allocation and content throttling, platforms effectively wield the power to reshape the "public agenda" without assuming the editorial responsibilities and public service obligations of traditional media. This constitutes a private power's encroachment on the public sphere, with its negative societal consequences borne by the public.

The algorithmic black box generates inherent risks that, as digital platforms serve as the core infrastructure for information flow, transaction matching, and social interaction, create systemic contagion risks, forming a "digital domino effect." When algorithms exhibit vulnerabilities, systems encounter security flaws, or are maliciously exploited by third parties (e.g., through large-scale cyberattacks, data breaches, or fraud exploiting platform weaknesses), the resulting risks rapidly propagate across the entire digital ecosystem and socio-economic systems. This transforms latent risks from linear accumulation into exponential growth and multidimensional infiltration, rendering traditional post-incident accountability and individual remedies inadequate. Therefore, requiring gatekeepers to assume stricter pre-incident obligations-such as enhanced security safeguards, algorithmic transparency, and risk assessment-directly embodies the imperative to internalize security costs.

3.2.2 Governance vacuum under the "quasi-public" attribute of the platform

The function of digital platform has gone far beyond the nature of "pure" commercial organization, and it has shown the attribute of "quasi-public". The platform is not only a trading place, but also an important carrier of information dissemination, social interaction and public service, and even undertakes the functions of market supervision, credit construction and dispute resolution, which are traditionally exercised by the government or public institutions.[20]

Through its user agreements, content moderation mechanisms, technical standards, and dispute

resolution rules, the platform establishes an effective "autonomous governance framework." This framework positions the platform as both a "legislator" and "enforcer" within its ecosystem-leveraging its technological advantages to transcend traditional intermediary roles, imposing constraints on market participants, and even de facto defining the boundaries of "public interest" in the absence of legal authorization or accountability mechanisms. Practices such as unilateral modifications to service terms, opaque content review criteria, arbitrary penalties (like account suspensions or speech bans), and decisions regarding content distribution or removal all demonstrate varying degrees of the distortion and expansion of "private subject power." However, at its core, this remains profit-driven commercial behavior lacking public law legitimacy, transparency, and external oversight. Such dynamics make it relatively easy for platforms to abuse their private authority while pursuing maximum commercial gains, potentially harming user rights and public interests.[21]

In stark contrast, state public authority in the digital age struggles to comprehensively govern digital platforms. The platforms 'massive scale, rapid iteration, hyper-connectivity, and global operations have created multiple regulatory challenges: "too many to manage" (due to their sheer numbers and diverse operations), "too fast to keep up" (with technology evolving faster than legislation), "too deep to see" (due to high technical barriers and data black-boxing), and "too new to comprehend" (as emerging risks diverge from traditional perceptions). This makes it difficult to establish effective, sustained oversight in the ever-changing digital ecosystem. Consequently, platforms create "regulatory arbitrage" opportunities in critical sectors or operate in unregulated "lawless zones." China's "govern the internet, internet governs users" strategy partially acknowledges platforms 'governance capabilities while recognizing that platforms alone cannot manage all risks. [22] Therefore, it emphasizes platforms' "primary responsibility" -a formal response to their "quasi-public" nature. In this sense, expanding gatekeeper obligations is not just a competition policy tool but also part of the state's grand institutional project to achieve effective governance and rebalance public-private power boundaries in the digital era.

3.3 Multiple Value Drives: Rebalance of Efficiency,Equity and Sustainability

For decades, antitrust law has been profoundly shaped by the Chicago School, with its core value prioritizing "efficiency" and often measured by "consumer welfare" maximization. Yet the complexity of the digital economy has starkly revealed the inherent limitations of this unilateral value paradigm, driving a regulatory revolution to rebalance efficiency, fairness, and sustainable diversity objectives.

3.3.1 Fair weighting: From transaction results to competition process

The traditional paradigm maintains that platforms need not intervene excessively, even when their exclusive practices harm some merchants, as long as they provide consumers with "free" or low-cost services. This "price-centric theory" has proven ineffective in the zero-price market where "data is money," systematically overlooking the "processual injustice" of platform power over two key groups.

The first issue is the "unfair transactions" faced by commercial users on the platform. Leveraging its monopoly over critical resources, the gatekeeper platform charges high commissions to small and medium-sized merchants, shifts their operational costs, and even restricts their business freedom through MFN Clauses, resulting in excessive value concentration within the platform itself. The expansion of gatekeeper obligations aims to shift regulatory focus from end-user pricing to ensuring fairer transactional relationships between the platform and commercial users by prohibiting unfair pricing and eliminating discriminatory clauses.

Secondly, there exists an "imbalance of opportunity" for potential competitors. The Chicago School once argued that "large corporations typically secure market positions through efficiency advantages, with their economies of scale and scope effects contributing to greater social welfare," thus advocating against hasty intervention. However, digital economy practices demonstrate that the "size" achieved by platforms through super network effects, data dominance, and "killer acquisitions" does not solely stem from efficiency gains. On the contrary, such "size" may also be attained by marginalizing potential competitors, stifling innovation, and erecting market barriers. Consequently, the new

regulatory paradigm no longer equates "size" with "quality" by default. Instead, it focuses on protecting the diversity of innovation ecosystems through open ecosystems and mergers and acquisitions regulation, ensuring the inherent openness and fairness of market competition.[23]

3.3.2 The manifestation of autonomy: From "consumer" to "digital citizen"

The expansion of gatekeeper obligations also redefines user roles. Users are no longer merely "consumers" chasing low prices, but have evolved into "data producers" and "digital laborers" who contribute data and shape the ecosystem-where their behavioral data becomes the platform's core asset. The traditional paradigm overlooks the numerous "non-price damages" caused by platforms when offering "free" services, including privacy violations, information cocoons, and deprivation of choice.

Through bundled services, default settings, and data migration restrictions, the platform systematically undermines users' autonomy in personal information management, creating algorithmic exploitation. The new regulatory framework emphasizes core rights including data portability, the right to uninstall pre-installed software, and opposition to opaque algorithmic manipulation. These obligations fundamentally transform users from passive "algorithmic subjects" into active "digital subjects" who control their data and digital destiny, safeguarding their fundamental autonomy as digital citizens.

3.3.3 Sustainable vision: From short-term efficiency to long-term prosperity

The emphasis on "fairness" and "autonomy" ultimately points to a grander value goal: the long-term sustainability of markets. A digital ecosystem dominated by a few giants, stifled by innovation, marked by wealth inequality, and where user rights are ignored-though it may exhibit short-term "concentration efficiency" -has an unstable and unsustainable foundation. The expansion of gatekeeper obligations signifies that antitrust regulation is shifting from short-sighted efficiency calculations to a long-termist concern for market ecosystem health. This means sacrificing some monopoly profits and control rights of platforms in exchange for greater innovation vitality, structural resilience, and social trust in the digital economy.[24]

4. Structured Path of Digital Platform Gatekeeper Responsibility Shaping

Effective regulation of platform power requires moving beyond traditional rule enumeration to adopt a more systematic and adaptive responsibility framework. This framework, centered on "Adaptive Governance," constructs its responsibility system through three dimensions of platform power issues: collaborative interventions in competitive order, public governance, and pluralistic values. This approach ensures effective constraints and constructive guidance of platform power.

4.1 Responsibility for Maintaining the Order of Competition

4.1.1 The negative list and the strong declaration of small merger and acquisition

To effectively combat anti-competitive practices by digital platforms exploiting their quasi-regulatory status and establish clear behavioral boundaries, we recommend adopting the EU Digital Markets Act (DMA) as a model. Specifically, for platforms designated as gatekeepers, a comprehensive list of prohibited activities should be explicitly defined (see Table 1). By implementing a negative list approach, this methodology avoids the time-consuming and costly case-by-case analysis inherent in traditional antitrust law. Through typified and proactive measures, it can prevent platforms from abusing their market dominance at the source.[25]

Table 1. Prohibited Practices for Digital Platform Gatekeepers

Category of behavior	Core Prohibited Points / Behavior Description
self preference	Do not favor your own products/services or impose unfair rankings, displays, or access restrictions on third parties
forced bundling	Only when providing core platform services, users are forced to subscribe or register for other ancillary services
abuse of data competition	It is forbidden to use the non-public business data of commercial users in the platform to engage in self-competition.
limit external trade/ optimal	Restrict commercial users from promoting products or signing contracts outside the platform, or prevent them from offering better

offer	quotes to end users
Pre-installed software and default settings restrictions	Users cannot be restricted from uninstalling pre-installed software or changing default settings
Block user freedom of choice	Do not restrict end users from switching between services through technical or other means

For instance, the introduction of Mandatory Reporting of Minor Acquisitions is crucial to address covert anti-competitive tactics like "killer acquisitions". As exemplified by Germany's GWB10, even if the target company doesn't meet the financial thresholds for traditional merger notifications, if it operates in the digital sector or possesses data collection capabilities, and if the acquired entity could potentially become a future gatekeeper competitor, the gatekeeper platform must file a mandatory report with regulators prior to the merger. This measure grants regulators "prior knowledge rights" and "pre-merger assessment rights", enabling them to anticipate and intervene in potential damages to future competitive landscapes and innovation ecosystems before the transaction concludes. This effectively prevents the risk of "killer acquisitions" that could stifle startups at their inception.

4.1.2 Obligations regarding data portability and interface interoperability

To break the 'lock-in effect' caused by data monopolies and closed ecosystems in digital platforms, and to promote market openness and user freedom, gatekeepers must enforce mandatory obligations for data portability and interface interoperability.

The data portability obligation empowers end users to control data (both personal and non-personal) generated or provided on the Gateway Platform. It enables users or their authorized third parties to freely, conveniently, and continuously access such data from the platform for use in other platforms or services. This obligation aims to dismantle industry entry barriers created by platform data monopolies, ensuring fairer access to essential data resources for emerging market entrants and small and medium-sized enterprises (SMEs). By enhancing market competitiveness, it prevents the "winner-takes-all" effect. The EU Data Protection Regulation (DPR) has extended this obligation to commercial users, allowing them to transfer data on behalf of end users with their consent, effectively safeguarding existing data assets during platform migration.

The obligation of interface interoperability aims to dismantle technical barriers between different platforms or services, fostering open sharing within platform ecosystems. Gatekeeper platforms should be required to freely open their core interfaces for software or hardware, enabling third-party service providers, commercial users, and alternative service providers to interact effectively with their systems. For instance, social media platforms should be mandated to open access to non-numerical interpersonal communication interfaces, allowing interconnectivity between different messaging applications and reducing reliance on single platforms. Meanwhile, for critical "bottleneck facilities" like app stores and search engines, gatekeepers must provide commercial users with access channels under fair, reasonable, and non-discriminatory (FRAND) terms, while publishing transparent access rules and dispute resolution mechanisms. Essentially, this transforms the "essential facilities theory" of traditional antitrust law – a post-facto remedy – into proactive obligations that gatekeepers must fulfill in advance. This approach promotes platform ecosystem openness at its source, preventing platforms from exploiting their dual identity (as both infrastructure providers and market competitors) to engage in self-biased or exclusive practices.

4.2 Collaborative Responsibilities in Public Governance

In this dimension, the gatekeeper responsibility aims to promote the platform to internalize its externalities and assume the public governance coordination obligations that match its growing influence.[26]

4.2.1 Third-party algorithm transparency audit and reporting system

Conducting periodic third-party audits of core algorithms is essential for building the platform's intrinsic capacity for proactive governance. The audit scope should adopt a lifecycle perspective, systematically examining the legality and compliance of training data, the explainability of model architecture and logic, as well as the differential impacts on various user groups. By conducting a multi-dimensional analysis (technical, legal, and social dimensions), the platform can promptly address algorithmic biases or potential manipulation tendencies.

Through appropriate information disclosure, it can clarify the original design intent and actual performance of the algorithms to the public, thereby internalizing externalities under the guidance of public discourse and regulatory compliance.

Specifically, regarding the application of audit methodologies: First, at the technical level, platforms should master advanced methods such as model interpretability analysis, reverse simulation, and differential privacy testing to conduct scientific evaluations of core algorithms 'fairness and accountability without compromising commercial confidentiality. Second, within legal and ethical frameworks, platforms must assess algorithms' impacts on personal privacy, data security, and social equity, using empirical data to identify potential systemic discrimination, information cocoon effects, and manipulation risks. Platforms should undergo simultaneous spot checks by regulators on audit plans and results, while publishing concise and understandable audit report summaries to the public within reasonable limits. Third, to prevent audits from becoming mere formalities, regulators may collaborate with platforms to establish rectification commitments and follow-up evaluation plans, integrating "issue identification" and "correction implementation" into a unified governance cycle. This approach ensures platforms genuinely fulfill their public accountability obligations when handling massive user bases and data.

4.2.2 Trustee data sharing pool and public interface standards

To prevent data silos from exacerbating market monopolies and public governance gaps, establishing a "trustworthy data sharing pool" is a critical step. In this context, the Gatekeeper Platform serves a dual role as custodian and security manager: On one hand, it implements security measures for data classification and categorization, applying anonymization or differentiated privacy protocols to highly sensitive personal information, while establishing more flexible access mechanisms for aggregated data with relatively low sensitivity but high value, balancing privacy protection with practical needs for social research. On the other hand, it establishes an access application and review system to provide orderly data access channels for legally qualified research institutions, public sectors, or non-profit organizations, while setting clear disciplinary clauses for unauthorized data usage to prevent abuse and secondary leaks.

Beyond the shared pool, to enable third-party researchers and developers to efficiently utilize platform data, the platform could standardize and open access to core functional interfaces. This would allow social innovation entities to deeply integrate and conduct further research and scenario-based applications within legal compliance frameworks. Specifically, the platform could implement a unified identity authentication and permission management system to categorize user access levels based on data call frequency or depth requirements, while establishing reasonable traffic control policies to prevent malicious exploitation of interfaces. Additionally, by rigorously standardizing data formats, invocation protocols, and metadata labeling, the platform can enhance interface scalability and compatibility, lowering entry barriers for diverse research teams and technical [27] communities. While ensuring data security and user privacy, this approach will sustainably deliver high-quality data resources for public services and social innovation, facilitating the transition from a traffic monopoly to a collaborative partner role.

4.3 The Responsibility for Coordinating Multiple Values

4.3.1 Differentiated encryption mechanism for privacy protection and open sharing

Excessive protection hinders data flow and innovation, while over-openness may compromise user privacy. Gatekeeper platforms should prioritize adopting differentiated encryption technologies such as Homomorphic Encryption, Multi-Party Computation (MPC), and Zero-Knowledge Proof (ZKP). These technologies enable tiered encryption protection without decrypting raw data, tailored to data sensitivity, sharing objectives, and recipient identities, ensuring data remains "usable yet invisible." Furthermore, platforms should invest in developing and promoting privacy-enhancing technologies, establish corresponding technical standards and compliance guidelines, and guide the industry toward higher-level privacy protection and data-sharing compatibility models. This approach helps strike a practical balance between "data as a resource" and "data as a human right," avoiding the weaponization of privacy to stifle competition or promoting competition at the expense of privacy. Ultimately,

this fosters a dynamic equilibrium between efficiency and fairness.[28]

4.3.2 Compliance sandbox and proportional regulatory toolkit

The goal of the goalkeeper responsibility is to create a dynamic balance between innovation and risk prevention, and to realize the coordination of multiple values in a more flexible and adaptive way.[29]

The First, Establish a tiered regulatory framework. Develop clear, quantifiable criteria for identifying gatekeepers by evaluating dimensions such as revenue, active user base, market share, and data control capabilities. Platforms should be categorized into different tiers (e.g., super platforms, large platforms, medium platforms), with periodic reviews to adjust regulatory tiers based on their development, ensuring precise oversight. Implement differentiated obligations and responsibilities for platforms at different tiers: Super platforms handling "public opinion attributes" (e.g., social media) or "strategic sensitivity" (e.g., operating systems, cloud computing) should bear heightened public governance responsibilities (e.g., algorithm transparency, information authenticity obligations). Platforms involved in data-sensitive sectors like finance and healthcare must adhere to stringent data security and privacy protection requirements. For smaller platforms or those with weaker market influence but high innovation activity, adopt a lenient regulatory approach to reduce unnecessary compliance burdens.[30]

The second, In regulatory enforcement, priority should be given to behavioral remedies. Only when all behavioral remedies have been exhausted without restoring effective competition, when platform systemic violations persist despite repeated warnings, or when market structures have become severely entrenched, should structural remedies such as asset divestment or business spin-offs be considered with caution. The potential impacts on market efficiency, innovation ecosystems, and consumer welfare must be thoroughly assessed to ensure these measures are necessary and proportionate means to achieve competition objectives.

Third, establish a regular communication mechanism between regulators and platforms, utilizing soft tools such as compliance guidelines, administrative interviews, risk alerts, and industry self-regulation in daily oversight. [31] Platforms that severely breach gatekeeper obligations should face heavy fines or even management accountability, with stricter penalties like industry bans or credit sanctions considered when necessary to set clear boundaries for violations. This approach ensures sound governance of the platform economy, avoiding both "chaos when relaxed" and "stagnation when over-regulated."[32]

5. Conclusion

Large internet platforms leveraging data advantages often form monopolies through economies of scale and scope, undermining competition in digital markets. Traditional antitrust laws prove inadequate in regulating these digital giants. As the world's second-largest digital marketplace, China's digital governance framework will not only shape its domestic market but also influence international legal frameworks and global industrial development. This necessitates establishing a new governance paradigm that balances "innovation incentives" with "anti-monopoly safeguards." At its core lies a tripartite responsibility framework integrating "competition order maintenance," "public governance coordination," and "diverse value alignment." Beyond serving as a regulatory blueprint, this paradigm fundamentally redefines the power dynamics among state, market, and society in the digital age. The establishment of gatekeeper responsibilities signifies a regulatory evolution from "market-centric" approaches to a multi-dimensional framework balancing "data rights" and "public interests." Ultimately, it requires modern legal systems to recalibrate the "power-responsibility-rights" triad in cyberspace.

References

[1] Li Guicheng and Gao Jin, "The Representation, Generative Logic, and Regulatory Pathways of Platform Power in the Digital Economy Era," Journal of Henan Normal University (Philosophy and Social Sciences Edition), 2024, No.3, pp. 16-22.

[2] Zhang Shouwen, "Improving the Anti-Monopoly Law: Positioning, Orientation, and Principles," Journal of East China University of Political Science and Law, 2020, No.2, pp. 6-16.

[3] Dai, Qizhi,Understanding How Platform

Modularity Enhances Network Effects,Electronic Markets, Vol.33, p.40(2023).
[4]Xiao Yuxian, Suo Cheng, Zhang Shaotong et al., "Data Gatekeepers: Functions, System Framework, and Future Prospects," Management Review, 2024, Vol. 12, pp. 60-71.
[5] Franck J-U, Peitz M. Digital Platforms and the New 19a Tool in the German Competition Act ,SSRN Electronic Journal,vol.12,P.513 -528(2021).
[6] Yan Chi and Wang Xiaoli, "Analysis and Prospects of the 'Gatekeeper' System in the Digital Market Law", Information and Communication Technology and Policy, 2023, No.3, pp. 54-60.
[7] Xiao Mengli: "From Metaphor to Field: Reflections and Reconstruction of the 'Digital Gatekeeper' ", in China Law Review, No.2, 2024, pp. 139-156.
[8] Wang Jian and Wu Zongze, "Antitrust Enters a New Era: A Review of the U.S. House Judiciary Committee's' Digital Market Competition Survey Report'," Competition Policy Research, 2020, No.4, pp. 63-82.
[9] Tan Hongru&Xuezheng Chen,The No Surcharge Rule and Its Welfare Implication, International Review of Economics & Finance, vol. 89,p.1369-1384(2024).
[10] Meng Yanbei and Zhao Zeyu, "Rational Regulation of Super Platform Self-Preferential Behavior under Anti-Monopoly Law," Journal of Central South University (Social Sciences Edition), 2022, Vol. 1, pp. 70-82.
[11] Xiao Dongmei and Liu Xinxin, "The EU's' Digital Gatekeeper' Criteria and Their Implications," Journal of Xiangtan
University (Philosophy and Social Sciences Edition), 2024, No.4, pp. 44-52.
[12] Chen Fei and Pu Wenjie, "Digital Market Law: The EU's Institutional Approach to Regulating Digital Gatekeepers," European Studies, 2023, No.1, pp. 23-56.
[13] Lin Xiuqin, "On the Paradigm Shift of Anti-Monopoly in the Digital Economy: A Case Study of the EU's Digital Markets Act", in Intellectual Property, 2022, No.7, pp. 3-19.
[14] Pierre Larouche&Alexandre de Streel, The European Digital Markets Act: A Revolution Grounded on Traditions, Journal of European Competition Law & Practice, Vol.12, p.542-560(2021).
[15] Zhang Sulun, "The Dual Nature of Platform Enterprises and Antitrust Regulatory Responses: On the Establishment of China's' Gatekeeper' System," Hebei Law Journal, 2024, No.1, pp. 98-113.
[16] Xu Li, "Theoretical Issues and Path Selection of Digital 'Gatekeepers' Abusing Market Dominant Position," in *Renmin University Law Review*, 2021, No.1, pp. 308-329.
[17] Jiang Mobing, Luo Lian, and Lü Pin: "Do 'killer acquisitions' exist in China's digital platform enterprises? -An analysis of characteristics, motivations, and consequences," in Economic Theory and Economic Management, No.9, 2024, pp. 87-104.
[18] Zhu Zhanwei, "The Legislative Expression and Reflection of the Gatekeeper System under the Anti-Monopoly Perspective," in Local Legislation Research, 2023, No.1, pp. 51-63.
[19] Cheng Wei, "Theoretical Interpretation and Normative Shaping of Digital Platforms' Increased Obligations," in Learning and Exploration, 2024, No.2, pp. 62-71.
[20] Yang Dong and Li Zishuo, "Regulating Tech Giants: Re-examining Technological Power as a Factor in Determining Market Dominance," Academic Monthly, 2021, No.8, pp. 92-105.
[21] Li Jian and Yin Yuhan. Digital Gatekeeper Theory: Origins, Misinterpretations and Development. Social Science Research, 2024, Vol. 3, pp. 11-24.
[22] Liu Peng, "Regulating the Internet: The Rise and Logic of Third-Party Platform Regulation," Governance Research, 2021, No.5, pp. 51-58.
[23] Liu Yatian, Xu Heng, and Wang Xiaojie, "Theoretical Analysis of Data Sharing's Impact on Competition and Welfare in Digital Platforms," *Research on Financial Issues*, 2025, No.5, pp. 66-79.
[24] Dai Xin, Platform Responsibility and Social Trust, Journal of Law Science (Journal of Northwest University of Political Science and Law), 2023, No.2, pp. 82-97.
[25] Liu Quan, "On the Primary Responsibility of Internet Platforms," Journal of East China University of Political Science and Law, 2022, No.5, pp. 79-93.
[26] Hu Xiaohong, "The Construction of

'Gatekeeper' Obligations in China's Platform Economy under the Anti-Monopoly Law," Xuehai, 2023, No.2, pp. 164-172.
[27] Yang Qingwang and Wang Haiying, "The Legal Foundation and Institutional Construction of Power Regulation in Digital Platforms," Journal of Central South University (Social Sciences Edition), 2023, No.2, pp. 117-131.
[28] Zhang Qilin, Wang Xuhui, and Wu Yun, "The Dilemma and Countermeasures of Anti-Monopoly in the Platform Economy: An Analysis of the Mismatch Between Platform Ecological Monopoly and Platform Enterprise Regulation," *Finance and Trade Economics*, 2023, No.7, pp. 142-158.
[29] Li Ben and Xu Huanyan: "China's Plan: The EU's Regulatory Innovation on Digital Platform 'Gatekeepers' ", Journal of Shanghai University (Social Sciences Edition), 2023, No.5, pp. 105-119.
[31] Jin Meirong and Li Qian, "On the Evolution of the 'Gatekeeper' System and Its Implications for Enhancing the Primary Responsibility of Chinese Internet Platforms," Inner Mongolia Social Sciences, 2023, No.2, pp. 107-116.
[32] Cheng Zengwen, "Constructing the Pre-emptive Review Obligation of Platform Private Law from the Perspective of 'Gatekeeper' Responsibility," *Nanjing University Law Journal*, 2023, No.3, pp. 94-111.