CHINA'S MODEL AND IMPROVEMENT APPROACH OF THE DIGITAL GATEKEEPER SYSTEM

Liu Canhua

TABLE OF CONTENTS

CHINA'S MODEL AND IMPROVEMENT APPROACH OF THE DIGITAL GATEKEEPER SYSTEM

Liu Canhua[*]

Establishing a digital gatekeeper system represents a cutting-edge global issue aimed at enhancing the legal framework for platform governance. The European Union's Digital Markets Act has raised international discussions by introducing a systematic approach to the digital gatekeeper paradigm. China's digital gatekeeper legislation embodies distinct Chinese characteristics, including the delineation of gatekeeper obligations across various scenarios, complex institutional objectives, a diverse array of gatekeeper obligations, and the promotion of platform self-governance. However, China's approach faces several challenges, such as fragmented legal provisions, ambiguities in the definitions and scope of gatekeeper obligations, an overemphasis on substantive measures, and insufficiently specialized regulatory and punitive mechanisms. To comprehensively implement and enhance the digital gatekeeper system, it is essential to adopt a more systemic, procedural, and accountability-oriented approach. This involves achieving a systematic interpretation and coordinated application of rules from diverse legal sources, establishing a robust gatekeeper identification mechanism, and refining regulatory and punitive measures in accordance with the principle of proportionality. These efforts are essential for advancing the modernization of platform governance systems and enhancing governance capabilities.

I. INTRODUCTION

In the era of the digital economy, platforms have evolved into key market entities and gradually become the dominant form of economic organization.[1] Early internet platforms were primarily limited to specific domains, providing intermediary services for bilateral or multilateral users. However, with the rapid development of the platform economy, internet platforms have continuously expanded their business boundaries, integrated heterogeneous business activities, and adopted a 'self-operated + third-party-operated' business model. This model endows platforms with a dual role: they serve

* Assistant Professor at the Institute of Law, Chinese Academy of Social Sciences.

1 *See* THE GOVERNANCE AND LIABILITY OF INTERNET INTERMEDIARY, at 12 (Zhou Xuefeng & Li Ping eds., China Legal Publishing House, 2018).

as important channels for third-party enterprises to enter the market while also becoming direct competitors to these enterprises. At the same time, user base and market share of some popular platforms have grown exponentially, ultimately giving rise to a group of super-large platforms that exert substantial dominance over cyberspace and the digital economy. From a global perspective, the rise of these super-large platforms has brought numerous new governance challenges, particularly in areas such as market entry barriers, self-preferencing behaviors, user rights protection, and the fairness of platform decision-making.[2]

To address various issues caused by super-large platforms, countries around the world are exploring solutions. One emerging trend is to designate large internet platforms as 'gatekeepers' and impose special obligations on them. In June 2019, the Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the House of Representatives of the U.S. launched an antitrust investigation and evaluation of the four major tech giants—Facebook, Google, Amazon, and Apple—and published the *Investigation of Competition in Digital Markets*. The report explicitly identifies the four companies as 'gatekeepers' that control critical distribution channels, possessing infrastructure-like characteristics while a large number of businesses rely on these platforms to access users and markets. To address the potential problems caused by large platforms, the report proposes countermeasures in areas such as maintaining the order of digital market competition, improving antitrust laws, and strengthening antitrust enforcement. This regulatory approach has been further deepened in the *Digital Markets Act* (DMA) of the European Union (EU), which explicitly designates large online platforms meeting certain conditions as 'digital gatekeepers' under the law and imposes extensive legal obligations on them.

In terms of 'digital gatekeepers', some countries have also explored regulatory frameworks on it. For instance, the *Tenth Amendment to the German Act Against Restraints of Competition* (GWB) introduced article 19a, which regulates the conduct of enterprises with substantial cross-market influence to prevent abuse of market dominance. Besides, article 58 of *China's Personal Information Protection Law* (PIPL) marks the initiation of specialized legislation targeting large internet platforms, thereby establishing a distinct Chinese model of digital gatekeeper governance.

By comparing the legislative approaches to digital gatekeepers in China and the EU, we can better delineate the substantive content and

2 Ding Xiaodong, *On Legal Regulation of Very-Large-Scale Internet Platforms*, 1 Science of Law (Journal of Northwest University of Political Science and Law) 95 (2025).

defining characteristics of the Chinese model. This comparative analysis provides a foundation for refining China's gatekeeper regime and developing evidence-based recommendations for its implementation and reform.

II. COMPARING THE EU MODEL AND CHINA'S DIGITAL GATEKEEPER FRAMEWORK

In recent years, the legislative initiatives of the EU in the field of cyber and information law have raised attention due to the Brussels Effect.[3] From the *General Data Protection Regulation* (GDPR) to the *Digital Services Act*, the DMA, and the more recent *Artificial Intelligence Act*, EU legislation has profoundly influenced theoretical frameworks, practical implementations, and legal system reforms worldwide. A particularly notable development occurred on November 1, 2022, when the DMA was unanimously approved by all 27 EU member states and officially came into effect. This regulation reshaped the paradigm for regulating large platforms by instituting the digital gatekeeper system.[4]

A. Core Elements of the EU's Digital Gatekeeper System

The DMA establishes the digital gatekeeper system by imposing a series of specific obligations and regulatory frameworks on large internet platform service providers (hereinafter referred to as platform enterprises). The objective is to further shape a competitive order that aligns with the characteristics and dynamics of the digital market, building upon traditional competition law frameworks to ensure competitiveness and fairness within the digital marketplace. The digital gatekeeper system primarily comprises three core components: the gatekeeper identification mechanism, gatekeeper obligations, and regulatory and penalty measures.

1. Mechanism for Designating Gatekeepers. — The gatekeeper designation mechanism within the DMA ensures that only platform enterprises with significant market influence and potential risks are subject to the special regulatory scope of the digital gatekeeper system. This

3 Feng Yujun & Wei Hongguang, *Theories and Criticisms of the GDPR's 'Brussels Effect': An Analysis of Legislative Extraterritorial Influence*, 6 Journal of Yantai University (Philosophy and Social Science Edition) 24-34 (2023). Zhao Haile, *The Limits of the EU's 'Brussels Effect' in Digital Market Governance Rules and China's Response*, 6 German Studies 78-95, 148-149 (2023). Fang Xingdong, Zhong Xiangming & Xie Yongqi, *The 'Brussels Effect' and Institutional Innovation of Digital Governance in China*, 3 Media Observer 33-44 (2024) .

4 Fang Xingdong, Zhong Xiangming & Zhang Quan, *'Gatekeeper' of Gatekeeper: Paradigm Shift of Global Governance in Cyberspace*, 1 Journal of Social Science of Hunan Normal University 49 (2023).

mechanism consists of the criteria for gatekeeper designation and the procedural framework for identification. Selecting large platform enterprises that meet specific conditions from the pool of all internet platform companies is fundamental to establishing the digital gatekeeper system.

The DMA delineates three substantive criteria for gatekeeper designation: significant impact, important gateway, and entrenched position. Significant impact refers to a company's considerable influence within the internal market; important gateway signifies that the core platform services provided by the company serve as a crucial gateway for business users to reach end users; entrenched position means that the company occupies an entrenched and durable position in its operations, or is expected to do so in the near future.

The term 'core platform services' refers to digital services widely used by business users and end users that exhibit characteristics such as extreme scale economies, very strong network effects, an ability to connect many business users with many end users through the multisidedness of these services, lock-in effects, and a lack of multi-homing or vertical integration. The DMA outlines ten types of core platform services, including online intermediation services, online search engines, social networking services, video-sharing platforms, number-independent interpersonal communications services, operating systems, web browsers, virtual assistants, cloud computing services, and online advertising services.

In addition to specifying substantive and formal criteria, the DMA outlines a comprehensive gatekeeper designation procedure. The general procedure includes both voluntary self-declaration by enterprises and designation by the European Commission. Furthermore, special procedures are provided for enterprises that meet the threshold conditions but do not qualify as gatekeepers (exclusion procedures) and for those that do not meet the threshold conditions but still qualify as gatekeepers (inclusion procedures). The DMA also prescribes special legislative procedures for modifying the threshold conditions or related calculation methods.

2. Defined Obligations for Gatekeepers. — The obligations of gatekeepers constitute the core content of the gatekeeper system. The innovative aspect of the DMA lies in its requirement for digital gatekeepers to fulfill a series of obligations aimed at achieving its legislative objectives: promoting the competitiveness and fairness of the internal digital market within Europe. Based on these legislative goals, the obligations imposed on gatekeepers primarily involve prohibiting actions that undermine digital market competitiveness or introducing unfair practices, as well as implementing measures that support and enhance market competition and fairness. While the

DMA lists numerous obligations, the most significant include preventing data abuse, promoting data sharing, preventing the abuse of gateway positions, fostering interoperability, and enhancing the fairness and transparency of the digital advertising market.

3. Regulatory Measures and Penalty Structures. — To enforce gatekeeper obligations and ensure the effective implementation of other rules, the DMA outlines a series of regulatory and penalty measures. Regulatory measures include market investigation procedures, oversight of enterprise compliance with obligations and commitments, and violation investigation procedures. Penalty measures are tailored to different types of enterprise misconduct, imposing substantial fines. For instance, enterprises that intentionally or negligently fail to comply with gatekeeper obligations may be fined up to 10% of their global annual turnover for the preceding financial year. For repeat violations within an eight-year period, fines can reach up to 20% of their global annual turnover for the preceding financial year.

B. Main Components of China's Approach to Large Platform Governance

Similar to the EU and other jurisdictions, China has been actively exploring a distinctive governance model for large-scale platforms in recent years, driven by the rapid development of the digital economy and the rise of major platforms. In this process, China's legal framework and legal theories have been influenced to some extent by the EU's DMA. However, rather than adopting the EU's comprehensive and systematic approach wholesale, China has pursued a gradual and incremental path to constructing its digital gatekeeper system.

1. Special Obligations Under the PIPL. — Paralleling the gatekeeper system in the EU, China's PIPL, which was passed on August 20, 2021, and came into effect on November 1, 2021, was the first to stipulate special obligations for large internet platforms concerning personal information protection. Article 58 requires personal information processors that provide significant internet platform services involving a huge number of users and complicated business types shall perform four categories of special obligations: (1) Establishing a compliance system for personal information protection, including an independent oversight body mainly consisting of external members. (2) Developing fair platform rules clarifying personal information processing standards and obligations product or service providers on the platforms. (3) Suspending services to providers on the platforms violating laws on personal information. (4) Publishing regular social responsibility reports on personal information protection and accept public oversight.

2. Special Obligations Under the Regulation on the Protection of Minors in Cyberspace. — Drawing from the legislative experience of the PIPL, the *Regulation on the Protection of Minors in Cyberspace* (RPMC), passed on September 20, 2023, and effective on January 1, 2024, introduced six special obligations for large digital platform service providers. Article 20 of the RPMC requires providers with a substantial number of minor users or significant influence on minors to fulfill the following obligations: (1) In the design, development, and operation of digital platform services, prioritizing minors' physical and mental health development and conducting regular impact assessments. (2) Providing a dedicated 'minor mode' or 'minor section' to promote access to beneficial products or services for minors. (3) Establishing a compliance system for minors' online protection including an independent oversight body. (4) Developing fair platform rules, specifying protection obligations for product or service providers on the platform, and informing minor users of their rights and the remedies against any cyber infringement. (5) Terminating services to product or service providers that severely harm minors' well-being or violate their rights. (6) Annually publishing a social responsibility report on minors' online protection and accepting public supervision. Of these six obligations, the third to the sixth mirror the obligations laid out in the PIPL, while the first two were crafted specifically to address the particular needs of protecting minors.

3. Special Obligations Under the Regulation on Cyber Data Security Management. — The *Regulation on Cyber Data Security Management* (RCDSM), passed on August 30, 2024, and effective on January 1, 2025, further developed the special obligations for 'large platforms' defined as digital platforms with over 50 million registered users or over 10 million monthly active users, characterized by complex business models and data processing activities that significantly impact national security, economic operations, and other critical societal areas. Article 46 prohibits such platforms from: (1) misleading, deceiving or coercing users into processing platform-generated data; (2) unreasonably restricting user access to their data; (3) implementing discriminatory practices harming user rights; or (4) engaging in other activities prohibited by laws or regulations.

Although the specific term 'digital gatekeeper' has not yet been employed in relevant Chinese laws and regulations, and there are viewpoints opposing the introduction of this concept into Chinese law,[5] if we define the

5 Zhai Zhiyong, *The Origin and Legal Basis of the Concept of Digital Gatekeepers*, 1 Jingchu Law Review 81 (2024).

digital gatekeeper system as a framework that stipulates special obligations and related matters for large platforms, it may be argued that China has, in fact, established a digital gatekeeper system. This system is primarily constituted by one law and two administrative regulations. Comparative legal studies on digital gatekeeper system between China and the EU reveal both similarities and distinct characteristics. Furthermore, while many rules within the EU's digital gatekeeper system may not be directly applicable to China, they nonetheless provide significant references for the implementation and further refinement of China's gatekeeper system.

III. DISTINCTIVE CHARACTERISTICS AND CHALLENGES OF CHINA'S DIGITAL GATEKEEPER SYSTEM

The establishment of a digital gatekeeper system is currently at the forefront of global network governance discussions. Due to varying national legal traditions, the development status of digital economies, and societal concerns, digital gatekeeper systems across different countries would inevitably exhibit significant differences. Compared to the EU's digital gatekeeper framework, China's system demonstrates unique characteristics in terms of legislative techniques, objectives, and specific provisions. However, this system also carries inherent risks and potential concerns.

A. Emphasizing Scenario-Specific Responsibilities for Large Platforms

The EU's DMA aims to promote the harmonization of laws across member states, while simultaneously limiting the legislative authority of individual nations in the domain of digital gatekeepers. To achieve this, the DMA establishes a comprehensive and systematic digital gatekeeper framework. From a logical perspective, this system appears robust. However, whether it aligns with the national circumstances and practical needs of individual member states remains uncertain. In contrast, China's digital gatekeeper legislation is not driven by a similar motivation, nor is there an urgent need for a comprehensive and systemic digital gatekeeper framework at present. Therefore, while recognizing the necessity of digital gatekeeper legislation, China adheres to a progressive approach, gradually developing the system. Specifically, in three distinct 'scenarios'—'personal information protection', 'minor protection', and 'cyber data protection'—China has introduced additional and special obligations for large platforms, which cumulatively form an evolving and systematic body of duties and regulations.

Article 58 of the PIPL marks the beginning of the legislative process for China's digital gatekeeper system. This article outlines several duties for digital gatekeepers, but does not directly address societal concerns such as new monopolistic behaviors or unfair competition by large platforms. Therefore, overall, the provisions remain incomplete. Some scholars have criticized these provisions as only 'half' of a digital gatekeeper framework.[6] In addition to the obligations outlined in the RPMC, the subsequent RPMC specifies a comprehensive range of duties throughout the design, development, and operation phases, including requirements to establish 'minor modes' or 'dedicated sections for minors'. These provisions serve to further enrich the content of China's digital gatekeeper system, ensuring a more robust and nuanced regulatory framework for the protection of minors online. Meanwhile, the RCDSM further advances the system by clarifying key concepts and introducing specific data processing obligations, enhancing operability and coherence.

Although the establishment of digital gatekeeper rules through three separate legal sources gives the system a fragmented appearance, the relevant provisions have covered key activities of large platforms, thus effectively forming a degree of systemic coherence. Additionally, it is important to note that, although the three laws and regulations pertain to distinct areas, and the criteria for identifying digital gatekeepers vary, in practice, the same large platform often meets the conditions set forth by all three legal sources. From this perspective, the three legal frameworks effectively target the same category of gatekeepers, requiring them to fulfill corresponding duties in different contexts.

However, it is undeniable that the legislative model of specifying gatekeeper obligations for different scenarios may pose some challenges for the implementation of the law, particularly regarding the maintenance of legal order and consistency. The PIPL, the RPMC, and the RCDSM differ in their standards for identifying large platforms, the types of obligations imposed on these platforms, and the responsibilities of regulatory authorities. This can lead to inconsistencies in legal interpretation and application. On the one hand, the decentralization of the legal framework increases the compliance costs for large platforms as they navigate multiple laws, potentially encountering conflicting obligations and responsibilities. On the other hand, different regulatory agencies may interpret and enforce these laws differently due to their distinct functions, which could lead to inconsistent

6 Zhou Hanhua, *Analysis of the 'Gatekeeper Clause' in the Personal Information Protection Law*, 5 Science of Law (Journal of Northwest University of Political Science and Law) 42 (2022).

enforcement standards. This inconsistency increases the arbitrariness of law enforcement and diminishes the predictability of enforcement outcomes for large platforms, ultimately undermining the uniformity of legal order.

B. Combining Comprehensive Legislative Objectives with Diverse Requirements

The DMA clearly defines itself as a regulation for the 'digital market', aiming to establish unified rules for the digital market to ensure that all businesses within the EU's digital industry operate in a competitive and fair market environment. This legislation not only improves the EU's competition law system but also, in a sense, achieves a paradigm shift in the antitrust approach to the digital economy.[7] It makes European digital market regulation more focused on providing substantial guarantees for fair competition in the European Digital Single Market.[8] Under this legislative objective, the DMA's gatekeeper obligations, though intricate, consistently focus on competitiveness. The specific obligations primarily prohibit actions that disrupt competition or undermine fairness and mandate measures that promote a healthy competitive order within the digital market. Thus, while the DMA's gatekeeper obligations are diverse in form, they fundamentally constitute a single category of competition law obligations. In contrast, China's gatekeeper system exhibits greater comprehensiveness, both in terms of legislative objectives and the content of obligations.

As to the legislative objectives, Chinese legislation pertaining to digital gatekeepers has been progressively expanding the scope of gatekeepers' obligations, thereby demonstrating that China's cyber governance prioritizes the regulation of large platforms as a fundamental supervisory strategy.[9] Since the rise of mobile internet, China has been committed to building a modern platform governance system. China's gatekeeper system serves the overarching goal of platform governance: by refining the legal norms governing large platforms, it further perfects the rule of law in a platform governance framework with unique Chinese characteristics and advances the modernization of both the platform governance framework and governance capabilities. Therefore, China's gatekeeper system differs fundamentally

7 Lin Xiuqin, *On the Paradigm Shift in Antitrust for the Digital Economy: Taking the EU Digital Markets Act as a Mirror*, 7 Intellectual Property 3 (2022).

8 *See* Zhao Jingwu, *From 'Super Large Platforms' to 'Gatekeeper Platforms': The Institutional Logic and Regulatory Characteristics of the EU's Digital Markets Act*, 2 Digital Law 206 (2023).

9 He Bo, *On the Improvement of China's Legal System for Online Protection of Minors*, 2 Science of Law (Journal of Northwest University of Political Science and Law) 108 (2024).

from the EU's DMA by pursuing multifaceted platform governance objectives beyond competition law.

As to the content of obligations, unlike the DMA's singular focus, China's framework incorporates diverse obligations addressing both state governance over platforms and platform self-regulation. Firstly, as part of state governance over platforms, the gatekeeper system mandates that large platforms fulfill 'direct obligations' to promote a healthy digital market order. A healthy order not only includes a fair competitive order, such as the data processing rules stipulated in article 46 of the RCDSM, which are comparable to relevant DMA provisions, but also encompasses other aspects of the order. For instance, the RPMC requires platforms to facilitate minors' access to beneficial and mentally healthy products or services within the platform, which aims to construct a digital market order that best serves the interests of minors.

Secondly, as part of platform self-governance, the gatekeeper system requires large platforms to fulfill 'third-party obligations'[10] to formulate reasonable platform rules and supervise user behavior within the platform. This raises a theoretical question: how to distinguish the third-party obligations of digital gatekeepers from those of ordinary platforms. From a formal legislative language perspective, there are no significant substantive differences between the two, leading to two interpretative paths. The first interprets the gatekeeper provisions as reiterating existing third-party obligations, emphasizing proactive compliance by large platforms. The second views these obligations as specialized requirements tailored to the unique characteristics of large platforms. To clarify this distinction, a doctrinal analysis is needed to explain the rationale, specific content, and detailed requirements of these specialized third-party obligations.

Lastly, beyond direct obligations and third-party obligations, both the PIPL and the RPMC require large platforms to publish annual social responsibility reports and undergo social supervision. Social responsibility is broader than legal obligations, encompassing legal compliance, user rights protection, public interests, and social contributions. However, neither the PIPL nor the RPMC provides a clear definition of social responsibility or the specific requirements for publishing social responsibility reports. This lack of clarity has led to inconsistent practices among platforms in fulfilling these obligations.[11] The RCDSM provides initial clarification

10 Gao Qinwei, *On Third-Party Obligations in Administrative Law*, 1 ECUPL Journal 40 (2014).

11 Chang Lin, Li Junhong & Yang Yangweiyi, *The Challenges and Practice of Social Responsibility Report of Personal Information Protection in Internet Industry*, 1 Information and Communication Technology and Policy 74 (2024).

through article 44, stipulating that social responsibility reports must include platforms' protective measures and their effectiveness, processing of user rights requests, and performance of externally dominated supervisory bodies, thereby focusing these reports primarily on demonstrating compliance with personal information protection obligations. By publishing social responsibility reports, platforms not only enhance their transparency and credibility but also systematically review and assess their compliance, thereby promoting self-regulation and continuous improvement.

C. Overemphasis on Substantive Rules

The fundamental logic of the digital gatekeeper system lies in selecting large platforms from numerous online platforms that exert substantial influence over cyberspace and imposing stricter legal obligations upon them. Accurately identifying these platforms is essential for constructing the legal framework. Challenges arise in defining the scope of digital gatekeepers: overly broad criteria may hinder digital market development, while overly narrow criteria may fail to achieve legislative goals and effectively supervise misconduct or illegal actions by large platforms.

To address this, the DMA not only establishes relatively clear substantive criteria for gatekeepers but also delineates detailed designation procedures, thereby creating a mechanism that integrates substance and procedure. This mechanism helps ensure that the scope of gatekeepers remains within a reasonable boundary, and that the designation process is scientifically and fairly conducted, and helps mitigate arbitrariness and uncertainty in the designation process.

In contrast, China's digital gatekeeper framework exhibits a substance-over-procedure characteristic. Specifically, the relevant legal provisions in China focus primarily on the substantive requirements for defining a digital gatekeeper and the substantive obligations imposed on them. The legislative emphasis lies on delineating a reasonable scope for gatekeepers and defining their obligations, while procedural requirements for designation are comparatively neglected, which may lead to the following two issues in practice.

1. Ambiguities in Gatekeeper Status Determination. — Without a formal procedural framework for gatekeeper designation, large platforms that meet certain conditions may be uncertain whether they qualify as gatekeepers. Such uncertainty increases compliance difficulties for large platforms. Due to the lack of a clear designation procedure, large platforms need to determine whether they qualify as gatekeepers in their compliance practices and thereby fulfill the relevant obligations. When platforms are uncertain about their status as gatekeepers, they might adopt one of two extreme strategies: either conservatively fulfilling all possible gatekeeper obligations to prevent regulatory risks, or rashly choosing not to fulfill relevant obligations to avoid increased compliance costs. Both scenarios are detrimental to achieving the ideal governance outcome for large platforms. The former may lead to unnecessary compliance burdens, while the latter may result in penalties for non-compliance.

2. Risks of Discretionary Abuse in Enforcement Practices. — In the absence of strict designation procedures, regulatory authorities may identify a platform as a digital gatekeeper in a simplistic or imprecise manner during regulatory or enforcement actions, and then assess whether there is a violation based on whether the platform has fulfilled its gatekeeper obligations. In this process, there is a lack of procedural safeguards for the involved large platform, especially as platform enterprises may not have adequate opportunities to defend or appeal the key issue of 'whether they qualify as digital gatekeepers'. This contravenes the basic principles of procedural justice and may lead to unjust enforcement outcomes. Designating a large platform as a digital gatekeeper undoubtedly involves significant interests of the relevant parties, and according to general legal principles, particularly procedural justice requirements,[12] strict decision-making procedures should be established for such matters, especially by granting the parties involved procedural rights, including the right to submit applications, hearings, defenses, cross-examinations, and appeals.

D. Prioritizing Platform Self-Governance over Administrative Penalties

Analogous to the EU's GDPR, the DMA imposes hefty fines on digital gatekeepers for violations or failures to comply, thereby urging these entities to meet their obligations under a rigorous regulatory framework. In contrast, China's digital gatekeeper system is characterized by a model that prioritizes platform self-governance, with regulation and penalties playing a supplementary role.

Firstly, while the PIPL specifies a range of administrative penalties for unlawful handling of personal information, including a maximum fine of 50 million yuan or 5% of annual turnover in article 66, its applicability to violations of article 58 is contentious and lacks clear interpretative consensus. The administrative penalties outlined in the PIPL target 'acts

12 *See* Mei Yang & Ye Shixiao, *The Application of the Principle of Due Process in Market Regulation and Law Enforcement*, 12 Research on China Market Regulation 35-40 (2023).

of processing personal information in violation of the provisions of this law, or failures to fulfill the obligations of personal information protection provided in this law.' However, as the gatekeeping obligations in article 58 do not explicitly pertain to the processing of personal information, whether a breach of article 58 could warrant penalties under article 66 remains theoretically debatable. Some scholars argue that article 58 solely regulates the management behavior of large platforms, rather than their handling of personal information; nevertheless, they also advocate for a broader interpretation of article 66 that would enable enforcement bodies to impose administrative penalties on large platforms that violate article 58.[13] This expansive interpretation has its logical challenges. Article 66 specifically targets unlawful personal information processing and failures to meet legal obligations during such processing. Thus, whether non-compliance with article 58 can be penalized under article 66 hinges on whether the violation relates to the platform's personal information processing activities. Specifically, three points arise: (1) While the first obligation outlined in article 58 pertains directly to personal information protection, it does not involve the processing of personal information but rather represents an internal corporate governance duty under company law to ensure compliance with personal information handling obligations. Consequently, a violation of this duty does not directly invoke article 66. (2) The second and third duties specified in article 58, which involve obligations towards third parties, do not concern personal information processing by large platforms, thus making them inapplicable under article 66 in cases of non-compliance. (3) The fourth obligation, which involves the publication of social responsibility reports, serves as a measure to ensure compliance with personal information processing obligations but does not directly pertain to specific personal information handling practices. Therefore, violations of this duty cannot directly invoke article 66 either. In summary, while the PIPL stipulates several gatekeeping obligations for large platforms, it lacks clear administrative enforcement measures. In this sense, these obligations currently hold an advisory rather than a mandatory nature.

Secondly, the RPMC provides explicit administrative penalty. This regulation outlines six duties, with varying levels of legal responsibility for non-compliance by large platforms. For violations of the first and fifth duties,

---

13 Yao Zhiwei, *The 'Gatekeeper' Obligations for Large Platforms in Personal Information Protection*, 2 Science of Law (Journal of Northwest University of Political Science and Law) 122 (2023).

the maximum administrative fine is set at 50 million yuan or 5% of annual turnover, while the maximum fine for other duties is capped at 1 million yuan. Although the regulation provides specific administrative penalties for failing to meet gatekeeping obligations, these measures remain relatively cautious in scope.

Lastly, the RCDSM does not specify penalties. Unlike the PIPL, the RCDSM adopts a formulaic approach to administrative penalties—'violating article XX of this Regulation shall result in administrative penalties of XX', but does not delineate corresponding administrative sanctions for breaches of article 46, which outlines the data processing obligations of large platforms.

In conclusion, China's digital gatekeeping regime currently emphasizes voluntary platform compliance over administrative penalties, aligning with national circumstances. First, platform autonomy is crucial for improving governance of the digital economy,[14] fostering cooperation with regulators, and promoting a fair and efficient digital market. Second, as the system is still evolving, it should focus on implementation and experience accumulation rather than strict measures. Third, the growth of large platforms is vital for the digital economy, so regulation should balance healthy development with behavior regulation. Unlike the EU's DMA, which imposes stringent penalties on foreign giants to protect local interests,[15] China aims to regulate large platforms to expand and strengthen the digital economy, nurturing more small and medium-sized platforms into large entities.

However, practice has demonstrated that legal obligations lacking punitive measures as a safeguard are often difficult to fully comply with and are easily circumvented by large platforms through flexible countermeasures or covert algorithmic rules.[16] Consequently, the authority of the regulatory framework is undermined, and the objectives of the system remain unfulfilled. Therefore, in the long term, it is essential to establish corresponding punitive measures for large platforms that violate gatekeeping obligations, based on the principle of proportionality and the objective needs of platform governance. This approach aims to encourage large platforms to more conscientiously fulfill their gatekeeping responsibilities.

14 *See* ESSENTIAL ELEMENTS OF PLATFORM ECONOMY, at 262 (Huang Yiping & Huang Zhuo eds., Peking University Press, 2023).

15 Chen Fei & Pu Wenjie, *Digital Markets Act: The EU's Institutional Path to Regulate Digital 'Gatekeepers'*, 1 Chinese Journal of European Studies 56 (2024).

16 Tang Yun, *The Responsibilities of Platforms in Protecting Minors Online and Their Implementation: A Discussion on the Enforcement of Article 20 of the Regulations on the Protection of Minors in Cyberspace*, 5 Children' Study 61 (2024).

IV. RECOMMENDATIONS FOR IMPLEMENTATION AND IMPROVEMENT

The digital gatekeeper system in China is still in its early stages of institutional development. Whether its rules can effectively achieve the intended objectives of the system remains to be tested in practice. On the one hand, the vitality of any system lies in its implementation. Therefore, efforts must be increased to strengthen the enforcement of the system, ensuring that legal rules are reasonably interpreted and applied in specific cases, and improving the supporting rules and safeguards for system implementation. This will help continuously enhance both the legal and social effects of the system's execution. On the other hand, the digital gatekeeper system is a nascent institution. As such, during its implementation, it is necessary to critically assess whether the relevant legal rules align with the system's objectives, are consistent with China's national conditions, and conform to the basic principles of platform governance. Issues arising in practice should be analyzed, and the duties of digital gatekeepers, along with the mechanisms for fulfilling these duties, should be gradually refined. This will contribute to the formation of a more mature and robust digital gatekeeper system.

A. Systematic Interpretation: Ensuring Coherence of Legal Provisions

China has initially constructed its digital gatekeeper system through several provisions in laws such as the PIPL, RPMC, and RCDSM, using a 'small-scale' approach, which could potentially result in conflicts between provisions, increasing the complexity of legal interpretation and causing uncertainty in law enforcement and judicial practice. For example, the third-party obligations under the digital gatekeeper duties require large platforms to fulfill management duties over platform users. However, these platforms might abuse their management power to restrict transactions or provide preferential treatment to their own business operations, violating the fairness principle of competition,[17] thus breaching the direct duties of the digital gatekeeper.

To address this issue, it is essential to adopt a systematic approach, interpreting and applying the relevant legal provisions of different laws

17 Liu Yun, *International Trends of Online Platform Antitrust and China's Response*, 6 Tribune of Political Science and Law 96 (2020).

and regulations with the mindset of 'one unified digital gatekeeper system' in order to enhance the rationality of rule application and the coordination between different rules. On the one hand, fragmented legislative arrangements do not necessarily imply fragmented interpretation and application. On the contrary, they require a systematic interpretation of the provisions from different laws and regulations, so that the provisions related to digital gatekeepers form a logically coherent system. This can prevent the coexistence of three separate gatekeeper systems due to the presence of three separate laws. On the other hand, from the perspective of legislative development, constructing a comprehensive and systematic digital gatekeeper system remains a key goal for future legislation. Systematic interpretation and theoretical approaches will provide necessary theoretical support for future systemic or even codified legislation.

Systematic interpretation is an important method of legal interpretation.[18] As for the current systematic interpretation of the digital gatekeeper provisions, it can be approached from the following three aspects:

1. Interpreting Different Legal Provisions with Unified Legislative Objectives. — Shared institutional objectives and values serve as the substantive guarantees for systematic interpretation and unified legal application. Although the specific content of different legal provisions and the duties of digital gatekeepers may vary, they should all serve the same legislative purpose: advancing the modernization of platform governance systems and governance capabilities. The Third Plenary Session of the 20th Central Committee of the Communist Party of China emphasized that the overall objectives of further deepening reform comprehensively is to continue to improve and develop the system of socialism with Chinese characteristics and modernize China's system and capacity for governance. The modernization of platform governance systems and governance capabilities is a key component of this overarching goal and is reflected throughout the PIPL, RPMC and RCDSM. Therefore, when interpreting and applying the provisions related to digital gatekeepers in these three laws, it is essential to ensure that the interpretative conclusions align with this institutional goal. In other words, through the value guidance of the institutional objective, consistency in the intrinsic values of the different digital gatekeeper provisions can be achieved, thus forming a unified system with a shared 'soul'.

18 *See* CLAUSE-WILHELM CANARIS, SYSTEMATIC THINKING AND THE CONCEPT OF SYSTEM IN JURISPRUDENCE: A CASE STUDY OF GERMAN PRIVATE LAW (2ND EDITION), at 92 (Chen Dachuang trans., Peking University Press, 2024).

2. Aligning Interpretative Conclusions with the Institutional Role of the Digital Gatekeeper System. — The digital gatekeeper system is a critical component within the broader platform legal framework. It is a specialized system designed in response to the practical issues and future concerns arising from the development of large platforms. Therefore, it is essential to accurately grasp the systematic position of the digital gatekeeper system, using the unique nature of the gatekeeper as a benchmark.

In particular, when interpreting the duties of digital gatekeepers, it is crucial to distinguish between the general obligations of platforms and the gatekeeper-specific duties of large platforms. Confusion in the classification of platform obligations may lead to negative consequences, such as an overly narrow or overly broad scope of obligated entities.[19] There may be both qualitative and quantitative differences between these obligations.

The 'qualitative distinction' lies in the fact that gatekeeper platforms are required to fulfill obligations that ordinary platforms are not. For example, while corporate social responsibility for ordinary platforms typically remains at the level of moral advocacy or 'soft law', gatekeeper platforms are legally mandated to publish social responsibility reports in areas such as minors' personal information protection. This transforms their corporate social responsibility obligations into enforceable 'hard law' requirements. Thus, the legal nature of social responsibility for gatekeeper platforms differs fundamentally from that of ordinary platforms, reflecting heightened regulatory expectations and stricter legal constraints due to their significant societal influence.

The 'quantitative distinction' refers to the hierarchical difference between gatekeeper platforms and ordinary platforms in fulfilling similar obligations. For example, all online platforms must achieve basic compliance as information processors, but gatekeeper platforms are required to establish a more rigorous compliance system and set up independent supervisory institutions. However, current legal frameworks have two key ambiguities: a lack of quantifiable standards for the institutionalization of compliance systems and the independence of supervisory bodies, and unclear guidance on whether compliance efforts can serve as grounds for exemption or mitigation of liability. To address these issues, a dual-track approach is recommended: establishing compliance benchmarks through guiding cases or departmental regulations, tailored to platform scale and business complexity,

---

19 Jin Meirong & Li Qian, *On the Transmutation of the Gatekeeper System and Its Enlightenment to the Perfection of the Subject Responsibility of Chinese Internet Platform*, 2 Inner Mongolia Social Sciences 114 (2023).

to prevent systemic risks in large platforms, while introducing a compliance effectiveness review mechanism in administrative enforcement. If gatekeeper platforms have implemented legally compliant systems and supervisory bodies but still violate regulations due to force majeure or novel risks, penalties should be mitigated or waived.

3. Unifying Conceptual Interpretations Across Different Legal Sources. — Regarding the specific provisions of the digital gatekeeper system, the PIPL, RPMC and RCDSM establish concepts and rules that are not entirely unified. To achieve a systematic interpretation and application, it is necessary to make coordinated efforts to harmonize or align the provisions of these three legal sources. A core example is the concept of the 'gatekeeper'. The EU's DMA has defined a unified concept of gatekeeper, whereas Chinese law does not use the term 'gatekeeper' but instead defines 'large platforms' in three distinct legal sources, each with different definitions. Therefore, the primary task of consistent interpretation is to determine a unified or coordinated definition of the digital gatekeeper across these different legal sources.

The earliest legal source to define the gatekeeper system, the PIPL, states that a 'digital gatekeeper' refers to a 'personal information processor providing significant internet platform services, with a large user base and complex business types'. However, it does not further clarify what constitutes 'significant platform services', 'large user base', or 'complex business types'. The RPMC defines a 'digital gatekeeper' as 'cyber platform service providers with a large number of minor users or platforms with significant influence on minors', but like the PIPL, it does not specify what 'large number' or 'significant influence' means. The regulation also stipulates that the Cyberspace Administration, in conjunction with relevant departments, will separately develop specific identification measures. Finally, the most recent regulation, the RCDSM, defines a 'digital gatekeeper' as a 'large cyber platform' and specifies the criteria for large platforms, which include having over 50 million registered users or over 10 million monthly active users, operating with complex business types, and having an impact on national security, economic operations, and people's livelihoods.

Thus, it is evident that the three legal sources differ in their descriptions of the criteria for digital gatekeepers, but when interpreting and applying the relevant rules, efforts should be made to achieve internal consistency in these provisions.

Firstly, all three sources emphasize the criterion of 'massive user base'. While the PIPL and the RPMC do not specify numerical thresholds, the RCDSM explicitly defines 'massive user bases' as platforms with 'over 50 million registered users or over 10 million monthly active users'. Applying the principle of systematic interpretation, we can conclude that only platforms meeting this numerical threshold satisfy the requirement of 'massive user base' under the PIPL and the RPMC. This approach ensures coherence across the legal framework while respecting the distinct regulatory objectives of each source.

Secondly, all three legal sources emphasize the significant influence of digital gatekeepers. While the wording varies—using phrases such as 'providing important internet platform services', 'having a significant impact on minors', and 'cyber data processing activities impacting national security, economic operations, and public welfare'—none of them provide clear criteria for determining 'significant influence'. Drawing on the experience of the EU's DMA, which explicitly defines core platform services through enumeration, this paper proposes that China's regulatory authorities adopt a similar approach. For instance, the DMA lists services such as online intermediation, search engines, social networking, video-sharing platforms, communication services, operating systems, web browsers, virtual assistants, cloud computing, and online advertising as core platform services. By issuing departmental regulations that enumerate specific types of 'important internet platform services', China could enhance the clarity and enforceability of its digital gatekeeper framework, ensuring consistency and coherence across legal interpretations and applications.

Lastly, both the PIPL and the RCDSM emphasize the complexity of the digital gatekeeper's business. Formally, business complexity refers to the provision of multiple types of services by the platform. For example, a platform might offer instant messaging, payment, social media, and live streaming services simultaneously. Substantively, business complexity refers to the influence of these services in their respective markets, creating a situation where switching platforms would incur significant costs for users. If a platform offers various services but only one service has a significant social impact, while the others have minimal influence, it would not meet the criteria of 'business complexity'.

B. Procedural Safeguards: Refining Rules for Fair Designation Process

The concept of a digital gatekeeper is employed metaphorically, vividly illustrating the pivotal role of large platforms in the digital era. However, such a metaphor inherently introduces conceptual ambiguity and uncertainty.

Consequently, the use of the 'gatekeeper' concept must be approached with caution to ensure the precision of its definitional scope and content.[20] In this regard, in the process of formulating the DMA, the EU has repeatedly amended relevant provisions concerning the constitutive requirements and identification procedures of digital gatekeepers.[21] However, it has consistently maintained the relative clarity of the definition and scope of digital gatekeepers by upholding a dual mechanism of substantive and procedural law.

In contrast, China's digital gatekeeper system currently exhibits an overemphasis on substantive elements while underappreciating procedural considerations. This imbalance partly reflects a legislative approach that needs more procedural thinking. Some may argue that the criteria for designating a digital gatekeeper are predominantly a matter of substantive law, with procedural mechanisms being less critical. However, since the determination of whether an online platform qualifies as a 'digital gatekeeper' significantly impacts the platform's major interests, it is imperative to establish a rigorous identification mechanism grounded in procedural law. Such a mechanism would enable specific large platforms to clearly ascertain their status as digital gatekeepers and provide appropriate legal frameworks to address disputes or exceptional circumstances that may arise.

Therefore, in the systematic development of China's digital gatekeeper system, it is necessary to reinforce procedural thinking and construct a robust gatekeeper identification mechanism. This integration ensures that the identification process is not only legally sound but also transparent and accountable, thereby enhancing the overall efficacy and legitimacy of the digital gatekeeper framework.

1. Establishing Transparent Procedures for General Gatekeeper Identification. — Identifying digital gatekeepers is not a straightforward task but a legal determination requiring adjudication, necessitating a rigorous identification procedure. In practice, the primary challenge posed by the digital gatekeeper system for large platforms is the uncertainty regarding their status as digital gatekeepers. Leading enterprises, in an effort to mitigate compliance risks, may choose to self-designate as digital gatekeepers and subsequently fulfill the associated legal obligations. However, for numerous companies, determining whether they qualify as digital gatekeepers remains

20 Wang Xuechun, *The Construction and Theoretical Evolution of the 'Gatekeeper' Concept—A Critique of Using 'Gatekeeper' as the Basis for Digital Platform Responsibility*, 1 Economic Law Review 135 (2024).

21 Zhu Yue, *Legislative Insights into EU Platform Governance: A Process Perspective on Comparative Law Research*, 3 Digital Law 191 (2023).

ambiguous, often placing them in a dilemma: self-designating as digital gatekeepers would increase compliance costs, whereas opting not to self-designate could expose them to penalties from regulatory authorities.

Nonetheless, instituting a comprehensive procedure to adjudicate the digital gatekeeper status of all online platforms would substantially escalate regulatory enforcement costs and from a governance perspective, such an approach is unnecessary. To address this, the EU's DMA has established a mechanism predominantly reliant on self-designation by digital gatekeepers, supplemented by regulatory confirmation. Specifically, if a company meets the constitutive criteria for digital gatekeepers—particularly thresholds related to revenue, user base, and other pertinent metrics—it is required to notify the regulatory authorities, who will then review and formally designate the company as a digital gatekeeper. Currently, the EU has officially designated seven companies, including Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and Booking, as digital gatekeepers through formal legal documentation.[22] Through this designation procedure, the DMA not only ensures the rigor of the digital gatekeeper designation mechanism but also enhances enterprises' predictability regarding enforcement and regulatory actions, thereby to some extent ensuring the scientific and effective nature of the platform governance framework.

2. Defining Procedural Standards for Special Case Designations. — The criteria for establishing digital gatekeepers are essentially a form of 'legal presumption'—enterprises that meet certain formal conditions are presumed to hold the status of digital gatekeepers. However, like most legal presumptions, these are not absolute; they are subject to exceptions, meaning they can be challenged and disproved.[23] Therefore, the digital gatekeeper mechanism should include a set of special procedures for handling exceptions. Specifically, these special procedures fall into two categories, corresponding to two types of exceptions.

The first category pertains to enterprises that, although formally satisfying the constitutive requirements of digital gatekeepers, do not substantively possess the status of digital gatekeepers due to certain special factors and thus are not required to fulfill all or part of the obligations of digital gatekeepers. For such special cases, it is necessary to establish specific exemption procedures, i.e., procedures to determine that an enterprise does

22 EUROPEAN COMMISSION, GATEKEEPERS, at https://digital-markets-act.ec.europa.eu/gatekeepers_en (Last visited on March 21, 2025).

23 Mu Zhiwei, *Analysis on Refutability of Legal Presumption*, 3 Journal of Kunming University of Science and Technology (Social Science Edition) 12 (2019).

not qualify as a digital gatekeeper or to decide to exempt a digital gatekeeper from fulfilling legal obligations.

The second category involves enterprises that, while not formally meeting the constitutive requirements of digital gatekeepers, possess special influence that effectively grants them the status of digital gatekeepers, thereby requiring them to fulfill all or part of the obligations of digital gatekeepers. This represents an expanded application of the digital gatekeeper system, necessitating the establishment of special identification procedures, i.e., procedures to determine that an enterprise, although not meeting the formal constitutive requirements, constitutes a digital gatekeeper, or to decide that a platform enterprise needs to fulfill certain gatekeeper obligations based on specific circumstances.

3. Introducing Mechanisms for Dynamic Adjustment and Periodic Review. — The status of digital platforms as gatekeepers is not fixed. Therefore, the designation of digital gatekeepers should be a dynamic process, requiring the implementation of adaptable identification procedures. On the one hand, due to factors such as market competition and changes in the national or global political and legal environment, the economic and social standing of online platforms within a country or worldwide frequently fluctuates. A digital gatekeeper enterprise may no longer meet the constitutive requirements of a digital gatekeeper due to a decline in status. To address this, the law should establish an 'exit mechanism': for situations where a digital gatekeeper no longer satisfies the constitutive requirements, corresponding procedures should be established for the digital platform to proactively apply for removal, regulatory authorities to conduct regular evaluations, and re-designation processes to ensure the reasonableness of the digital gatekeeper system throughout its entire lifecycle.

On the other hand, the status and obligations of digital gatekeepers are intrinsically linked to the services their platforms provide. Changes in the platform services offered by a digital gatekeeper can potentially affect its gatekeeper status and obligations. For example, a large platform initially designated as a digital gatekeeper may only fall under the category of a 'personal information processor', thereby being required to fulfill gatekeeper obligations under the PIPL. However, as its business expands and the number of minor users increases, it may evolve into a 'provider of online platform services with a significant impact on minors or a large number of minor users' under the RPMC, thereby necessitating the fulfillment of special gatekeeper obligations for the protection of minors. In such cases, it is necessary to establish dynamic adjustment procedures that dynamically modify the legal obligations the platform needs to fulfill based on the development of its business and changes in its influence.

C. Accountability Framework: Improving Regulatory and Punitive Measures

Strengthening the legal obligations of online platforms and intensifying the regulatory and punitive measures against platform violations have become a global legislative trend in the realm of internet law. However, the DMA has also been criticized for overregulation and hindering the development of the platform economy.[24] Given that the obligations of digital gatekeepers in China are relatively complex and that the regulatory objectives for digital gatekeepers do not entirely align with those of the EU, it is necessary to fully consider China's national conditions and practical needs when refining related regulatory and punitive measures.

1. Tailoring Regulatory and Punitive Mechanisms to the Complexity of Gatekeeper Obligations. — The diversity and complexity of digital gatekeeper obligations in China necessitate the development of differentiated regulatory and punitive responses based on the nature of the obligations violated. For violations of preventive obligations, regulatory and punitive measures should be relatively lenient. For instance, if a gatekeeper fails to establish external regulatory bodies, reasonably formulate platform rules, or publish social responsibility reports without causing substantial harm, less coercive measures such as official consultations should be prioritized to encourage self-correction. Administrative penalties should only be imposed in cases of severe violations or when substantial harm has occurred. Third-party obligation violations require nuanced assessment of the platform's contributory role, degree of control over offenders, and actual influence on harmful outcomes. Violations of 'direct obligations', such as unreasonable differential treatment of users that infringes upon their legitimate rights, should attract more stringent penalties. Such behavior represents a new form of consumer rights infringement in the digital age, and severe sanctions are necessary to prevent large platforms from exploiting 'new business models' to unlawfully profit, thereby safeguarding consumer rights and maintaining fair market competition.

2. Ensuring Proportionality in the Design and Application of Penalty Measures. — Punitive measures must uphold the principle of proportionality, ensuring that sanctions are commensurate with the severity of the violations.

---

24 DIGITAL GATEKEEPERS: ANALYSIS OF THE EU'S DIGITAL MARKETS ACT, at 15 (Ding Daoqin & Xia Jie eds., Law Press・China, 2023).

Once a doctrine rooted in administrative law to constrain police powers, the principle of proportionality has since evolved into a cornerstone of constitutional law, serving as a vital safeguard for rights and freedoms.[25] Globally, many countries have intensified penalties against large platforms in recent years. For example, in January 2023, the Irish Data Protection Commission imposed a €390 million fine on Meta for failing to provide consumers with non-targeted advertising options.[26] Due to cyber effects, violations by large platforms often infringe upon the legitimate rights of a vast number of users while generating substantial profits, making high fines proportionate to the societal harm caused by such violations. However, while increasing the severity of punitive measures, it remains necessary to reaffirm and adhere to the principle of proportionality, which helps prevent enforcement agencies from abusing discretionary power,[27] particularly by avoiding the imposition of high fines on gatekeeper platforms solely due to their large scale, and also by preventing tendencies toward profit-driven enforcement, thereby ensuring that punitive measures are just and reasonable.

A critical aspect requiring review is whether the administrative penalty provisions within the RPMC comply with the principle of proportionality. According to the RPMC, for violations of the six gatekeeper obligations, administrative penalties include 'orders to make corrections, give a warning, and confiscate the illegal gains; where the violator refuses to make corrections, a fine of not more than 1 million yuan shall be imposed thereupon.' For severe violations of the obligations to 'prioritize minors' physical and mental health development and conduct regular impact assessments' and to 'terminate services to product or service providers that severely harm minors' physical and mental health or violate their lawful rights', the penalties can include 'orders to make corrections, confiscate the illegal gains, and impose a fine of not more than 50 million yuan or 5% of the previous year's turnover, as well as orders to suspend relevant businesses, or suspend all the business operations for an overhaul, and notify the competent authorities to revoke relevant business permits or license.'

While the graduated administrative penalties nominally reflect the

25 Liu Quan, *Disputes and Reflections on the Application of the Proportionality Principle*, 5 Comparative Law Studies 172 (2021).

26 SCOTT IKEDA, IRISH DPC ORDERS €390 MILLION FINE TO META OVER TARGETED ADVERTISING, ORDERS IMPLEMENTATION OF ABILITY TO OPT OUT, at https://www.cpomagazine.com/data-protection/irish-dpc-orders-e390-million-fine-to-meta-over-targeted-advertising-orders-implementation-of-ability-to-opt-out/#:~:text=Ireland's%20Data%20Protection%20Commission%20has%20handed%20down%20a,its%20targeted%20advertising%20practices%20on%20Facebook%20and%20Instagram (Lasted visited on March 21, 2025).

27 Li Ben & Xu Huanyan, *Chinese Solution: Implications of the EU Innovative Regulation of Digital Platform 'Gatekeepers'*, 5 Journal of Shanghai University (Social Sciences Edition) 116 (2023).

requirement of the principle of proportionality, the substantial disparity between a 'fine of not more than 1 million yuan' and 'fines of not more than 50 million yuan or 5% of the previous year's turnover' creates an excessive gap, lacking intermediate levels. This discrepancy grants regulatory authorities overly broad discretionary power. Future legislation on the digital gatekeeper system should avoid similar frameworks. It is recommended to subdivide 'severe' circumstances into 'severe' and 'particularly severe' categories. Only in 'particularly severe' cases should fines of not more than 50 million yuan or 5% of the previous year's turnover apply, while 'severe' cases should incur fines of not more than 20 million yuan or 2% of the previous year's turnover. Additionally, to address the high fines associated with administrative penalties, a strict administrative discretion benchmark mechanism and a more rigorous administrative enforcement mechanism should be established to further limit administrative discretion and curb the frequent occurrence of 'maximum fines' in regulatory practice.

3. Integrating the Digital Gatekeeper System with Other Regulatory Frameworks. — Close attention must be paid to aligning the digital gatekeeper regulatory framework with existing regulatory systems to ensure seamless coordination and minimize the risk of overlap or conflict. This requires identifying areas of potential interaction, clarifying responsibilities, and establishing mechanisms for effective communication between regulatory bodies.

Firstly, the principle of non-duplication of penalties should be upheld to prevent excessive punishment. Large platforms may violate multiple legal provisions simultaneously while breaching gatekeeper obligations. For instance, if a platform's behavior infringes both gatekeeper obligations and specific personal information processing duties, it should adhere to the relevant provisions of the *Law on Administrative Penalty*, which prohibit imposing multiple fines for the same violation. Instead, the highest applicable fine should be imposed.

Secondly, it is essential to address the coordination between civil, administrative, and criminal liabilities. Digital gatekeepers who violate their gatekeeper obligations may be subject to corresponding civil, administrative, and even criminal liabilities. Given the particularities of the digital gatekeeper system, the primary legal responsibility for large platforms violating gatekeeper obligations is administrative rather than civil.[28] However, we should deeply consider how to innovate civil protection

28 Cheng Xiao, *Civil Liability of Large Network Platforms for Violating Gatekeeper Obligations*, 5 Science of Law (Journal of Northwest University of Political Science and Law) 41 (2023).

methods in the digital age to more effectively resolve disputes arising from digital gatekeepers infringing upon civil rights. For example, some scholars suggest establishing a system of joint liability with strict vicarious responsibility to ensure the deterrent effect of the digital gatekeeper system.[29]

At the same time, it is necessary to uphold the principle of minimal criminalization while strengthening regulation to prevent the premature intervention of criminal law in the digital gatekeeper system. For actions by digital gatekeepers that have serious social harms, they should be addressed in accordance with current criminal law provisions, adhering to the principle of legality in crimes and punishments, and avoiding arbitrary expansive interpretations or the *ad hoc* creation of new offenses.

Thirdly, it is essential to properly manage the relationship between administrative supervision and judicial intervention. Judicial institutions and administrative agencies play distinct roles in the implementation of the digital gatekeeper system. As a general principle, it is necessary to adhere to the principle of maintaining a constant overall regulatory intensity: in areas where administrative supervision is insufficient, higher-intensity judicial intervention is required, whereas in situations where administrative supervision is strong and effective, judicial bodies should exercise restraint.[30] Currently, the Chinese digital gatekeeper system does not emphasize the unique role of the judiciary. In the future, while enhancing the administrative regulatory mechanisms, it is also imperative to fully leverage the judiciary's role in interpreting laws in individual cases, constraining regulatory power, and establishing precedent-setting cases.

V. CONCLUSION

The DMA has established the EU model for governing large platforms by implementing a stringent digital gatekeeper system that imposes clear obligations and regulatory measures on major digital platform enterprises. As large platforms increasingly influence various aspects of China's economy and society, China also faces an urgent need to regulate large internet platforms. However, China's relevant legislation has not adopted the EU's 'leap forward' approach or 'codification' strategy. Instead, it has constructed the preliminary form of China's digital gatekeeper system through multiple legal sources.

29 Sun Zhaohang & Du Yanlin, *Study on the Introduction of 'Gatekeepers' for Digital Platforms*, 2 Science Technology and Law (Chinese-English Version) 105 (2024).

30 Xiao Mengli, *From Metaphor to Field: Reflection and Reconstruction of the 'Digital Gatekeepers'*, 2 China Law Review 155 (2024).

With the gradual implementation of China's digital gatekeeper system and the evolving development of the platform economy in China, the digital gatekeeper system still needs to undergo timely reforms and enhancements. The Third Plenary Session of the 20th Central Committee of the Communist Party of China emphasized that the overall objectives of further deepening reform comprehensively are to continue to improve and develop the system of socialism with Chinese characteristics and modernize China's system and capacity for governance. The reform and development of China's digital gatekeeper system must serve the realization of this overarching goal, particularly by enhancing the system's comprehensiveness, procedural integrity, and accountability. This involves continuously advancing the modernization of the platform governance system and governance capacity in the digital age from these three dimensions, thereby formulating a Chinese solution for the digital gatekeeper system.

(Edited by Gong Li)

数字守门人制度的中国模式与完善路径

内容提要 构建数字守门人制度是完善平台治理法律体系的前沿议题。欧盟数字市场法创造的体系化数字守门人制度产生了世界性影响。中国数字守门人立法有着明显的中国特色，包括分场景规定数字守门人义务、制度目标复杂、守门人义务种类多元、倡导平台自我治理，但也存在法律规则碎片化、守门人义务内涵与外延不清晰、重实体轻程序以及专门性监管处罚措施不足等隐忧。全面实施和健全数字守门人制度，要加强体系思维、程序思维和责任思维，实现不同法律渊源规则的体系化解释和协调适用，建立健全守门人认定机制，完善符合比例原则的监管处罚措施，以推进平台治理体系和治理能力现代化。