

---

Original Research Article

## From traditional compliance to digital transformation: Innovation in building and practical pathways for antitrust compliance systems

Yajun Wang<sup>1</sup>, Haishui Yan<sup>2</sup>

*1 Senior Partner, Deputy Director, Capital Equity Legal Group (Shanghai), Shanghai, 201199*

*2 Chairman of the Board, Zhonghe Digital Union (Beijing) Technology Co., Ltd., Beijing, 102218*

---

**Abstract:** In the context of the rapid development of the national digital economy, the rise of the platform economy, accompanied by potential monopoly risks, poses a severe challenge to the traditional antitrust compliance system. This paper begins with an analysis of national antitrust policies and regulatory trends, explaining the limitations of traditional compliance models in addressing issues in the platform economy era. By exploring the role of digital technologies such as big data, artificial intelligence, cloud computing, and privacy computing in driving compliance transformation, the paper points out that digital empowerment can facilitate the transition from static post-event regulation to dynamic, real-time early warning systems and intelligent auditing. Based on typical platform enterprise case studies and the experiences of small and medium-sized enterprises using SaaS compliance tools, this paper summarizes feasible models and optimization strategies for digital compliance. It also addresses implementation challenges such as technical barriers, data privacy protection, talent development, and policy standard improvement, proposing strategies for multi-dimensional collaboration and industrial ecosystem building. The study concludes that the construction of a digital compliance system helps improve the precision and efficiency of national antitrust regulation and internal corporate compliance, laying a solid foundation for the fair, transparent, and sustainable development of the platform economy.

**Keywords:** Antitrust Compliance; Digital Transformation; Algorithm Auditing; Big Data Regulation; Data Governance

---

### 1. Introduction

Over the past decade, the national digital economy has flourished, with internet platform enterprises at the core of an expanding industrial ecosystem. This ecosystem now encompasses diverse digital industries, including e-commerce, online payments, transportation services, social media, online entertainment, food services, and delivery services. However, in this process, platform enterprises, driven by network effects and rapid accumulation of data resources, often gain strong market positions in specific sub-markets, potentially forming or leading to monopolistic structures. This can harm the legitimate interests of other market participants and reduce overall market innovation and resource allocation efficiency. Therefore, how to effectively conduct antitrust regulation and ensure corporate antitrust compliance has become a critical issue in the digital economy era.

In the traditional industrial era, antitrust compliance mainly focused on monitoring and punishing relatively straightforward behaviors such as price agreements, capacity restrictions, and market division. Compliance practices relied heavily on legal texts, manual inspections, and post-event investigations. However, in the digital economy era, compliance requirements are vastly different. Firstly, the market power in platform economies is often data-driven and algorithm-supported, with competition strategies no longer limited to simple pricing but incorporating precise recommendations, dynamic pricing, differentiated services, and algorithm-

driven business logic. Secondly, the opacity and complexity of data resources, user profiles, and algorithmic decisions make it difficult for traditional methods to quickly identify and effectively curb anti-competitive behavior. In this context, relying solely on traditional compliance tools and regulatory methods can no longer meet the demands of the era, making the construction of a new antitrust compliance system based on digital methods and enhanced real-time monitoring and early warning capabilities essential.

At the national regulatory level, there has been a strengthening of antitrust enforcement and policy guidance in the platform economy sector. For example, the Antitrust Law revision emphasizes enforcement details specific to platform economies, encouraging multi-dimensional regulatory frameworks in areas such as algorithms, data, and platform structures. At the same time, regulatory agencies have signaled the use of digital technologies to improve enforcement accuracy, aiming to more efficiently identify monopolistic behavior with limited resources. For enterprises, there is an urgent need to transform from traditional compliance models to digital solutions: on the one hand, to use digital compliance tools to achieve comprehensive, dynamic monitoring of business processes, supply chains, and market behaviors; on the other hand, to establish internal mechanisms for data compliance, algorithm auditing, and privacy protection to meet the rapidly changing policy environment and regulatory requirements.

This study aims to explore the innovative construction and practical pathways for antitrust compliance systems in the context of digital transformation. Specifically, it will analyze how digital technologies (such as big data, artificial intelligence, cloud computing, and privacy computing) can empower compliance. Based on case studies and industry practices, this study will attempt to outline a digital antitrust compliance framework and provide implementation suggestions for platform enterprises and regulatory agencies to reference during compliance transformation.

The research method involves literature review, systematically analyzing recent antitrust cases and regulatory trends in the platform economy sector in China, while also incorporating international practices and regulatory guidelines to establish a comparative perspective. Furthermore, typical cases from national platform enterprises and third-party compliance service providers will be analyzed to examine the effectiveness and challenges of using digital tools for identifying monopolistic risks and improving compliance efficiency. Finally, the paper will propose countermeasures and suggestions to address the data governance, cost, and talent challenges enterprises may face during digital transformation.

Through this study, we aim to answer the following questions:

1. Why does antitrust compliance practice need digital transformation in the digital economy era?
2. How can digital technologies empower antitrust compliance systems by providing new solutions in data governance, algorithm auditing, and information sharing?
3. How should enterprises and regulatory agencies collaborate to build an efficient compliance ecosystem, achieving precise regulation and flexible compliance?

The significance of this study lies in providing strategic insights for platform enterprises, policymakers, and third-party service providers. On the one hand, enterprises can learn how to use digital compliance tools to proactively identify and prevent potential monopolistic behaviors, reducing compliance costs and enforcement risks. On the other hand, regulators and industry associations can draw on these experiences to develop more detailed and actionable digital regulatory policies and compliance guidelines. Moreover, the study offers practical examples for the academic community to consider antitrust compliance issues from legal, economic,

and technological perspectives, contributing to deepening research in this area. In the following chapters, the study will systematically discuss the foundational system, the logic of digital empowerment, practical cases, challenges, and policy recommendations, offering feasible pathways for constructing a new antitrust compliance system.

## **2. The Institutional foundation of antitrust compliance and challenges in the digital age**

### **2.1. Review and characteristics of the traditional antitrust compliance model**

Traditional antitrust compliance practices stem from the market regulatory logic of the industrial economy era. During this period, the market structure was relatively clear, with production materials, sales channels, and transaction behaviors being fairly transparent. Market power for businesses was primarily reflected in their control over prices, capacity, and distribution networks. The main tools for antitrust compliance included:

- 1. Legal provisions and post-event review:** Regulatory agencies relied on explicit antitrust laws and regulations, investigating and punishing clear anti-competitive behaviors such as monopoly agreements, price-fixing, and market division to ensure market competition was not overly distorted.
- 2. Offline data and manual judgement:** Compliance reviews depended on traditional information sources, such as written documents, financial data, and business contracts. Regulators would study and compare the evidence item by item to determine whether a company had abused its dominant market position or engaged in horizontal monopoly behavior.
- 3. Passive and periodic supervision:** Compliance practices were more oriented toward responding to inspections, lacking continuous, dynamic self-checking tools. Internal compliance departments would typically take action only when external investigations began or when regulatory authorities issued investigation notices.

While this model was somewhat suitable for the economic and technological environments of its time, its limitations became increasingly apparent with the rise of the internet and the platform economy. Information asymmetry and the exponential growth of data make it difficult for regulators to identify potential monopoly risks at the right time and level. Enterprises also face challenges in using traditional tools to self-inspect and preemptively address complex online transactions, dynamic pricing, recommendation algorithms, and other new phenomena.

### **2.2. National antitrust policy and regulatory trends**

With the country's economic transformation and the widespread use of internet technologies, there has been a gradual increase in attention to and regulation of the platform economy at the policy level. After years of implementing the original **Antitrust Law**, the country began to take more forceful enforcement actions against monopolistic behaviors in the digital economy. Recent policy and regulatory trends include:

- 1. Strengthened platform economy regulation:** In investigations and penalties against large internet platforms, regulators have emphasized that platform enterprises must not use data and algorithmic tools to engage in unfair competition or abuse market dominance. Stringent control of practices like "choice restriction" reflects a zero-tolerance attitude at the policy level.
- 2. Focus on algorithms and data governance:** Regulatory policies are increasingly concerned with algorithm transparency and data usage boundaries, requiring platforms to eliminate "black box" risks in

key areas such as pricing, recommendations, and traffic distribution.

3. **Balancing innovation and fairness:** While enforcing the law, regulatory agencies aim to avoid overly stringent, one-size-fits-all interventions. They encourage businesses to continue innovating within a compliant framework. At the same time, policy guidance and industry standardization are accelerating to ensure a clearer and more predictable compliance environment.

Compared to the traditional market structure, the platform economy exhibits significant network externalities and economies of scale. The market share and user loyalty of a few leading enterprises are exceptionally high, which makes it challenging for regulators to balance promoting innovation and maintaining fair competition. Moreover, due to the complex nature of data, algorithms, and platform ecosystems, regulation must continuously upgrade its strategies and incorporate technological means to adapt to new forms of competition.

### 2.3. New challenges in the digital age

The characteristics of the digital age — vast amounts of information and rapid data transmission — present new challenges for antitrust compliance:

1. **Challenges in data volume and quality:** Today, platform enterprises collect data from sources such as user behavior logs, transaction records, social interactions, and location tracking, resulting in volumes, speeds, and dimensions of data far exceeding those in the traditional economy. Regulatory agencies must adopt efficient data processing and analysis methods to handle such massive and heterogeneous data. At the same time, enterprises must establish data standardization, cleaning, and analysis systems to ensure the effective flow and timely early warning of information.
2. **Algorithmic black boxes and hidden behavior:** Traditional monopolistic behaviors, such as price-fixing and market division, often had clear written agreements or publicly available pricing information. However, monopolistic behaviors in the platform economy may be hidden within complex algorithmic logic. Companies can manipulate search rankings, traffic distribution, and pricing mechanisms via algorithms, marginalizing competitors in the view of users. This hidden behavior greatly complicates compliance reviews, requiring both regulatory authorities and internal compliance teams to employ technology to audit algorithms and trace and explain their outcomes.
3. **Cross-industry and cross-regional regulatory challenges:** Digital platforms often span multiple industries (e.g., payments, logistics, content distribution) and regions, making it difficult for traditional regulatory models, which are based on industry or regional divisions, to adapt. Furthermore, the self-sufficient supply chains within platform ecosystems may reduce the competitive opportunities for new entrants, requiring a systemic and holistic approach to antitrust regulation.
4. **Real-time regulation and dynamic compliance needs:** The pace of change and decision-making cycles in the digital economy are much faster than in traditional industries. Price adjustments, changes in traffic allocation strategies, and other decisions can be made within short periods, potentially altering market dynamics. This means that regulation and compliance cannot solely rely on post-event actions but must be capable of dynamic, real-time monitoring and response. Digital compliance tools can perform both early warning during the event and tracing afterward, providing quick and effective decision support to both businesses and regulators.

The challenges of antitrust compliance in the digital age are not only technical but also involve upgrades in

institutional design, regulatory thinking, and corporate governance models. Traditional methods overly rely on post-event penalties, manual judgments, and offline processes, whereas the competitive landscape in platform economies requires compliance practices to shift from passive to proactive, from point-based judgments to full-process monitoring, and from isolated departments to information sharing. While national regulators have begun to tighten enforcement and refine policies, there is still considerable distance to establishing an efficient, transparent, and sustainable digital antitrust compliance system. Against this backdrop, digital empowerment and compliance innovation have become key themes of shared concern for industries, academia, and regulators. The next chapters will focus on how digital transformation can provide new momentum and practical pathways for antitrust compliance.

### 3. The logic and pathways of digital empowerment in antitrust compliance

Faced with the complex competitive landscape and monopoly risks in the digital age, digital technologies are providing new tools and strategic pathways for antitrust compliance. Emerging technologies such as big data, artificial intelligence, cloud computing, and privacy computing enable both enterprises and regulators to shift from traditional static, delayed, and manual compliance methods to dynamic, real-time, and intelligent compliance ecosystems.

#### 3.1. Data-driven risk identification and early warning mechanisms

In the digital economy, data is not only the core asset of platform enterprises but also a key resource for identifying monopoly risks. Both enterprises and regulators can establish data-driven risk identification and early warning mechanisms in the following ways:

1. **Data standardization and cleaning:** Standardizing and cleaning internal data ensures that data generated across business processes can be uniformly retrieved, analyzed, and compared, thus providing a high-quality data foundation for compliance detection.
2. **Machine learning and anomaly behavior detection:** Using text mining, clustering analysis, and time series prediction techniques, enterprises and regulators can analyze transaction data, user feedback, and price fluctuations to quickly identify suspicious pricing strategies, unusual transaction concentrations, or imbalanced traffic allocation.
3. **Dynamic early warning models:** Real-time data stream processing technologies can be used to build dynamic early warning models. Once indicators such as market concentration, price elasticity, or user retention rate trigger warning signals, the system can promptly notify the enterprise's compliance team and decision-makers, enabling intervention and adjustment before the issue spreads.

#### 3.2. Algorithm auditing and result tracing

Potential monopolistic behaviors in the digital economy are often realized through hidden algorithmic logic. To achieve more precise antitrust compliance monitoring, it is essential to introduce algorithm auditing and result tracing mechanisms:

1. **Algorithm transparency:** Regular audits of platform companies' core algorithms are necessary, requiring companies to provide algorithm explanation documents, model architecture, and parameter explanations. This ensures that regulatory authorities and compliance consultants can understand the decision logic behind algorithms.

2. **Interpretable models and a/b testing:** Using interpretable machine learning models, enterprises can conduct A/B tests to compare recommendation results and pricing strategies, verifying whether the algorithm is biased, maliciously excluding competitors, or engaging in price discrimination.
3. **Building algorithm auditing tools:** Developing compliance detection plugins or algorithm auditing systems allows for regular data output collection from key decision points on the platform. These tools can reverse-analyze algorithmic outputs to identify potential monopoly signals.

### 3.3. Cloud computing and saas compliance tools deployment

For many small and medium-sized platform enterprises, building a complete digital compliance system is cost-prohibitive. In this case, cloud computing and Software-as-a-Service (SaaS) compliance tools offer cost-effective and efficient solutions:

1. **Scalable cloud platforms:** Compliance reviews, risk identification, and data analysis modules can be deployed on cloud platforms, enabling enterprises to scale computing resources up or down according to their business size, reducing reliance on local hardware.
2. **One-Stop compliance saas products:** Third-party compliance technology service providers can offer SaaS solutions that include modules for antitrust reviews, algorithm testing plugins, and compliance document management tools. Enterprises can subscribe to these services, obtaining continuously updated compliance capabilities without the need for additional development or maintenance costs.
3. **Cloud platforms for collaboration between regulators and enterprises:** Regulatory agencies may use cloud platforms to establish data exchange and monitoring interfaces with enterprises, enabling real-time sharing of compliance information. This would contribute to the creation of a more transparent and efficient regulatory ecosystem.

### 3.4. Balancing data governance and privacy protection

In digital compliance, data governance and privacy protection are critical components. As regulatory standards for platform data usage become clearer, enterprises must ensure compliance and security when acquiring, storing, and processing data:

1. **Privacy computing technologies:** Privacy-preserving technologies such as homomorphic encryption and federated learning can be used to allow regulators and compliance analysts to perform risk assessments without exposing sensitive raw data. This ensures user privacy while satisfying compliance inspection needs.
2. **Data classification and access control:** A data classification and management system should be established within the platform. Sensitive data should be subject to strict access control and de-identification processing, ensuring that data is used appropriately within the compliance process.
3. **Cautious cross-border data transmission compliance:** For enterprises involved in cross-border business, it is necessary to comply with cross-border data transmission regulations. Enterprises should file and monitor data transfer processes, utilizing digital tools to ensure traceability and control of data transmission across borders.

### 3.5. Collaborative governance and multi-party participation in compliance ecosystem building

The effective promotion of digital antitrust compliance requires multi-party collaboration:

1. **Collaboration between internal compliance departments and technical teams:** Compliance staff should collaborate with data scientists and algorithm engineers to embed compliance requirements into the design of business and product processes, ensuring proactive prevention.
2. **Collaboration between government, industry associations, and third-party service providers:** Regulatory agencies can work with industry associations and technology providers to establish digital compliance standards and technical guidelines, providing benchmarks and reference models for enterprises implementing digital compliance.
3. **Building a compliance information sharing platform:** Through trusted digital platforms, enterprises and regulators can exchange compliance information, encouraging industry self-regulation and collective learning, which helps to reduce the costs of duplicate efforts.

The introduction of digital technologies provides a new logic and implementation pathway for antitrust compliance: transitioning from post-event static reviews to real-time warnings and dynamic adjustments, from relying solely on manual judgments to intelligent identification and explainable algorithm audits, and from individual compliance upgrades to industry collaboration and ecosystem building. Under the specific regulatory environment and industry layout of the country, this digital empowerment transformation not only improves compliance efficiency and precision but also lays the foundation for fair and orderly competition, contributing to the healthy development of the industry.

## 4. Case studies and practical pathways exploration

After establishing the logic and pathways of digital empowerment in antitrust compliance, specific case studies and practical experiences can further verify the feasibility and effectiveness of this approach. The following examines the current application of digital transformation in antitrust compliance, based on national platform enterprises' compliance practices and cross-industry comparisons.

### 4.1. Digital compliance practices in typical platform enterprises

1. **Compliance exploration in large e-commerce platforms:** A large e-commerce platform, facing increasingly stringent regulation, began building an internal data monitoring and algorithm auditing system. By deploying compliance detection tools on the cloud, the platform integrates vast amounts of product pricing, sales data, and user feedback into a unified analysis framework to monitor price fluctuations and merchant ranking changes in real-time. Once signs of abnormal concentration or synchronized price changes are detected, the system automatically alerts the internal compliance team for further investigation. To enhance algorithm transparency, the platform also established a dedicated algorithm audit team to regularly inspect recommendation engines, search rankings, and traffic distribution algorithms, ensuring there is no favoritism toward self-operated stores or exclusion of competitors.
2. **Dynamic regulation pilot in a ride-hailing platform:** A ride-hailing platform worked closely with regulatory authorities to establish a data interface that enables the regulator to periodically access critical data on ride orders and pricing strategies. Internally, the company uses machine learning models to analyze price variation curves, fleet distribution, and order response times in specific regions. If signs of price irregularities, unfair dispatching, or traffic bias are detected in any area, the internal system immediately blocks the relevant algorithmic strategies and triggers compliance reviews. This practice

not only improved the platform's sensitivity to potential monopoly risks but also provided regulatory authorities with more direct data support, reducing enforcement delays caused by information asymmetry.

#### 4.2. Small and medium-sized enterprises using third-party compliance saas tools

In contrast to large platform enterprises, small and medium-sized digital platforms often face limitations in resources and technical capabilities. As a result, they are more inclined to adopt third-party compliance SaaS services. For example, a technology service provider offers a compliance monitoring plugin for small e-commerce businesses, which is embedded into the merchant's backend system. Once the merchant subscribes to the service, they can view pricing fluctuations, search ranking changes, and competitive landscape analysis reports from a unified interface, enabling them to identify potential compliance risks early. Such tools can also provide data encryption and privacy protection solutions to ensure that user rights are not violated during compliance checks. This greatly reduces technical barriers and compliance costs for small businesses, enabling them to have digital compliance capabilities comparable to those of large platforms.

#### 4.3. Cross-industry comparison and experience sharing

1. **E-commerce and content distribution platforms:** E-commerce platforms focus their compliance efforts on price regulation and merchant resource allocation, while content distribution platforms (such as short videos and news aggregation services) primarily face issues like algorithmic recommendation bias and monopolistic information suppression. The former relies more on price and sales data for digital monitoring, while the latter tends to audit recommendation logic using interpretable AI models to ensure that content exposure is fair and that no malicious suppression of competitors occurs. Both types of platforms require algorithm audits, but they focus on different aspects. This provides insights for cross-industry regulation and offers valuable lessons for enterprises in different sectors.
2. **Ride-hailing and online payment sectors:** The focus of ride-hailing platforms is on real-time price control, dynamic scheduling, and regional monopoly monitoring, while online payment platforms are more concerned with transaction fees, payment channel prioritization, and user data compliance. Despite the differences in sectors, both industries face the challenge of ensuring strict data governance in their digital compliance, ensuring that transaction and pricing information is traceable, and decision-making logic is transparent. The experiences in the ride-hailing and payment sectors show that by introducing cloud computing and data analytics technologies, data across different processes can be effectively integrated, allowing for timely detection and correction of monopolistic behavior.

Looking at the cases and industry practices, it is clear that digital compliance is gradually becoming an industry trend. Enterprises have significantly improved their sensitivity to potential monopoly problems and their response speed by introducing scalable technology tools, establishing internal auditing processes, and enhancing interactions with regulators. These practices not only provide practical references for improving digital compliance systems but also lay the foundation for regulatory bodies to further refine compliance standards, data interfaces, and technical guidelines.

### 5. Implementation challenges and countermeasures

Although digital empowerment offers new possibilities for antitrust compliance, challenges related to

technology, cost, privacy, and regulatory coordination remain during implementation. To promote this process smoothly, multi-dimensional countermeasures and suggestions are necessary.

### 5.1. Technical and cost barriers

1. **Technical deficiencies and cost pressures in small and medium enterprises:** Some small platforms lack professional data analysis teams and technical resources, making it difficult to introduce AI, cloud computing, and other compliance tools in the short term. In this case, governments and industry associations could consider establishing public compliance technology service platforms to offer basic compliance review tools and data analysis support at a low cost for small enterprises.
2. **Standardized Interfaces and Modular Tool Development:** Promoting the formulation of compliance data standards and the development of modular compliance tools can unify data processing tools across different enterprises and sectors. This reduces the difficulty of integrating internal systems and improves the universality and scalability of compliance tools.

### 5.2. Balancing data privacy and compliance

1. **Improving regulations and technical standards:** Governments and regulatory agencies should introduce more detailed standards for data privacy protection and compliant data usage, guiding enterprises to collect, process, and analyze data according to regulations. Clear punitive and corrective mechanisms should be in place for enterprises that misuse data.
2. **Technological empowerment of privacy protection:** Encouraging the use of privacy-preserving technologies such as privacy computing and blockchain traceability in compliance checks will allow for compliance and risk analysis to proceed without violating user privacy. Through encrypted computation, data de-identification, and verifiable blockchain records, digital compliance can move forward in an orderly manner without compromising user rights.

### 5.3. Compliance culture and talent development

1. **Cultivating cross-disciplinary talent:** Digital compliance requires collaboration across legal, technical, and data analytics fields. Enterprises should focus on cultivating interdisciplinary talents who understand both legal regulations and have data processing and technical knowledge. Internal training and assessment systems should be established to support this.
2. **Incorporating compliance awareness into corporate strategy:** Compliance should not be viewed merely as a passive response to regulatory requirements or a means to avoid penalties but should be integrated into the long-term strategic planning of the enterprise. Senior management should emphasize compliance building and prioritize digital compliance as part of the innovation and development agenda, ensuring that the compliance team has the necessary resources and authority.

### 5.4. Policy guidance and industry ecosystem optimization

1. **Regulatory sandboxes and pilot projects:** Regulatory agencies should establish compliance sandboxes to provide a space for businesses to innovate with digital compliance tools and models. By accumulating experience from pilot projects, successful compliance solutions can be expanded for broader implementation.
2. **Collaborative industry chain and public service platforms:** Industry associations, technology

alliances, and regulatory bodies should work together to build public data and compliance service platforms. These platforms could provide algorithm auditing services, case libraries, and standards, reducing the difficulty for enterprises to build their own compliance systems. Additionally, promoting cooperation mechanisms for compliance data exchange and risk early warning between upstream and downstream enterprises will facilitate collaborative governance.

Through the implementation of multi-level countermeasures, the barriers to digital antitrust compliance are expected to gradually diminish. Technology and cost issues can be alleviated through standardization, modularization, and public service platforms; privacy and data protection challenges can be addressed through regulatory guidance and technological innovation; and the construction of compliance talent and culture will provide internal momentum for the long-term sustainability of digital compliance.

## 6. Conclusion and outlook

This paper explores the challenges and opportunities faced by antitrust compliance in the digital economy era, discussing the logic and practical pathways for reshaping compliance systems using digital technologies. In the specific regulatory environment and industry context of the platform economy, digital transformation offers the following key insights:

1. **Digital technologies can help shift from passive post-event regulation to dynamic, real-time monitoring and early warning systems.** Through big data, machine learning, and algorithm auditing tools, enterprises can detect potential monopolistic behavior faster, and regulators can intervene more quickly, reducing the duration of market distortions.
2. **The practical pathway for digital compliance is already emerging:** Large platforms have built relatively mature compliance systems through internal data governance and algorithm auditing, while small enterprises have rapidly enhanced their compliance capabilities by using third-party SaaS tools. Industry-specific case studies show that the digital compliance model can be applied across sectors but must be customized for different industry characteristics.
3. **Achieving digital compliance is not an overnight process.** Challenges related to technology costs, talent shortages, data privacy, and policy standards still exist. Through policy guidance, public service platform construction, and industry chain collaboration, enterprises can lower technical barriers, standardize data usage, and create a more favorable compliance ecosystem.
4. **Digital compliance systems will continue to evolve towards greater intelligence and ecosystem integration.** With the deeper application of explainable AI, blockchain, and privacy computing technologies, the precision and transparency of compliance tools will continuously improve. On the international stage, countries may engage in compliance technology standardization and experience sharing to enhance their influence in global digital compliance discussions.
5. **Digital empowerment provides a new direction and implementation pathway for antitrust compliance.** This transformation not only helps maintain a fair and orderly market competition environment but also lays the long-term foundation for the healthy development of the national digital economy. Through continuous technological innovation, policy improvement, and industry collaboration, national antitrust compliance systems will evolve toward greater flexibility, transparency, and efficiency.

## **References**

- [1] Xiaoye W. The Theory and Practice of Antitrust Regulation in China's Digital Economy. *Journal of the Chinese Academy of Social Sciences*, 2022(5):31-48.
- [2] Shengli L, Xiaoqi Q. Optimization of Antitrust Administrative Sanctions in the Platform Economy Era. *Economic Law Review*, 2022(1):18.
- [3] Bing C. The Risk of Algorithmic Collusion in the Digital Economy and the Regulatory Path of Antitrust Laws. *Law Forum*, 2024, 39(4):80-90.
- [4] Zanjin Q. The Historical Evolution and Rational Approach of Platform Economy Antitrust—Taking 'Choose One' as an Example. *Financial Theory and Practice*, 2024, 45(2):154-160.