**Sarhad Journal of Legal Studies**
ISSN: 3106-7441 (Print) 3106-745X (Online)
January-June 2026, Vol. 02, No. 01, [32–41]
Published: 31st March 2026
Publisher: Sarhad Institute of Legal Studies, SUIT
https://journal.suit.edu.pk/index.php/sjls
**RESEARCH PAPER**

# Trade Secrets as 'Important Data' IP: A Comparative Study of Legal Risk in Sino-US Data Transfers

**Aamir Akhtar[1*] Li Lingfeng[2] Umar Farooq[3]**

## ABSTRACT

The rapid digitalization of global commerce has intensified legal conflicts over the control and transfer of intellectual property (IP)-related data. This article examines the irreconcilable tension between China's Data Security Law (DSL) and Personal Information Protection Law (PIPL) and the extraterritorial reach of the US CLOUD Act. It argues that China's data sovereignty framework classifies commercially sensitive information such as source code, AI training data, and R&D outputs as "Important Data," subject to stringent security assessments and strict controls on cross-border transfers. In particular, Article 36 of the DSL functions as a blocking provision, prohibiting disclosure of domestically stored data to foreign authorities without state authorization. Conversely, the US CLOUD Act empowers law enforcement agencies to compel US-based service providers to produce data regardless of its physical location, effectively extending US jurisdiction beyond national borders. This creates a legal paradox in which compliance with one regime results in violation of the other. The article demonstrates that this regulatory conflict generates significant legal uncertainty and operational risk for multinational corporations. It concludes that, in the absence of harmonized global standards, data localization and geofencing remain the most viable short-term compliance strategies.

**Keywords:** Trade Secrets, Important Data, Cybersecurity Law, Data Localization Policies, Data Security Regulation, Confidential Business Information.



## INTRODUCTION

The rapid digitalization of the global economy has fundamentally transformed the role of data, placing high-value corporate intellectual property (IP) at the center of cross-border regulatory conflict. Information that once flowed relatively freely across jurisdictions is now increasingly subject to competing legal regimes, particularly between the United States and the People's

[1] LLM Scholar, School of IP Law, Zhongnan University of Economics and Law, Wuhan, China; (aamirakhtar500@gmail.com) **(Corresponding)**
[2] ZUEL-SUR, School of Law and Economics, Zhongnan University of Economics and Law, Wuhan, China; (18826355156@163.com)
[3] Advocate, District Bar Association Lahore, Pakistan; (umerkamboh700@gmail.com)

Republic of China (PRC). Within this evolving landscape, corporate trade secrets such as proprietary algorithms, research and development (R&D) data, technical specifications, and artificial intelligence (AI) training datasets have emerged as both critical economic assets and highly vulnerable forms of data. For multinational corporations (MNCs), the management of such trade secret data is no longer merely a matter of internal governance or contractual protection. Instead, it has become a strategic compliance challenge shaped by conflicting national laws. Industries such as biotechnology, financial services, and advanced manufacturing depend heavily on the secure cross-border movement of sensitive data. However, the legal environment governing these flows has become increasingly fragmented, exposing firms to significant regulatory risks. At the center of this conflict lies a fundamental divergence in legal philosophy. China has developed a comprehensive data governance framework grounded in the principle of data sovereignty, primarily through the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). Under this framework, commercially sensitive information may be classified as "Important Data," subject to strict regulatory controls, mandatory security assessments, and limitations on cross-border transfer. Article 36 of the DSL operates as a blocking provision, prohibiting the disclosure of domestically stored data to foreign judicial or law enforcement authorities without prior government approval.

In contrast, the United States has adopted an extraterritorial approach to data access through the Clarifying Lawful Overseas Use of Data (CLOUD) Act. This legislation enables U.S. law enforcement agencies to compel disclosure of electronic data from U.S.-based service providers, regardless of where the data is physically stored. As a result, data located within China may still fall within the jurisdictional reach of U.S. authorities if it is considered to be under the "possession, custody, or control" of a U.S. entity. The interaction between these two regimes creates a structural legal conflict that can be described as a "Legal Catch-22." Compliance with a valid order under the U.S. CLOUD Act may constitute a direct violation of Chinese law, while adherence to China's blocking provisions may expose corporations to penalties under U.S. law. This situation places MNCs in an untenable position, where legal compliance in one jurisdiction necessarily results in non-compliance in another.

Despite growing academic attention to cross-border data regulation, much of the existing literature focuses on personal data protection, particularly in relation to frameworks such as the European Union's General Data Protection Regulation (GDPR). Comparatively less attention has been given to non-personal data, especially trade secrets, which form the backbone of the modern digital economy. The classification of such data as "Important Data" within China's legal framework further intensifies the regulatory uncertainty and expands the scope of state control over commercially sensitive information. This paper addresses this gap by examining the legal risks associated with the cross-border transfer of trade secret data between China and the United States. It conducts a comparative legal analysis of the Chinese data sovereignty framework under the DSL and PIPL and the extraterritorial enforcement regime of the U.S. CLOUD Act. The study evaluates the resulting compliance challenges faced by multinational corporations and analyzes the practical implications of conflicting legal obligations.

The remainder of this paper is structured as follows. Section two reviews the relevant literature on data sovereignty and cross-border data governance. Section three outlines the research methodology. Section four presents the comparative analysis of the Chinese and U.S. legal frameworks and examines the resulting Legal Catch-22. Section 5 concludes by discussing the broader implications and potential pathways toward regulatory coordination.

## LITERATURE REVIEW

### *Data Sovereignty and the Chinese Regulatory Model*

Existing scholarship on cross-border data governance highlights the emergence of data sovereignty as a central principle in China's regulatory framework. The Chinese approach treats data not merely as an economic resource but as a strategic national asset subject to state control. The Data Security Law (DSL) and the Personal Information Protection Law (PIPL) reflect a comprehensive legal architecture that integrates economic governance with national security objectives (Kostka & Antoine, 2022; Liu, 2023). Under this framework, data generated or stored within China falls under the authority of the state, representing a shift from sector-specific regulation to a centralized governance model. Scholars have noted that this approach differs significantly from Western systems, which emphasize market efficiency and individual privacy. Instead, China's model incorporates regulatory oversight, national security considerations, and economic strategy into a unified structure of data governance (Luo & Zhao, 2022). The Cyberspace Administration of China (CAC) plays a central role in implementing this framework, with authority to regulate, monitor, and assess data flows. This institutional structure reinforces the state's ability to control data as both an economic and security resource, reflecting a broader policy orientation toward digital sovereignty and strategic autonomy.

### *The Concept of "Important Data" and Regulatory Uncertainty*

A key feature of China's data governance framework is the classification of "Important Data," which encompasses information that may affect national security, economic stability, or public interests. However, the absence of a precise statutory definition has been widely identified as a source of regulatory uncertainty. Instead of a fixed definition, sectoral authorities and regulatory bodies retain discretion in determining what constitutes Important Data (Wu, 2023). This ambiguity has significant implications for multinational corporations (MNCs), particularly those handling commercially sensitive information such as trade secrets, source code, and research and development (R&D) data. Scholars argue that such information is increasingly likely to fall within the scope of Important Data, especially when it relates to strategic industries or cross-border operations (Gao, 2023; Zhou, 2023). The discretionary nature of classification creates a compliance environment characterized by uncertainty and risk. Companies may only discover that their data is classified as Important Data retrospectively, exposing them to regulatory scrutiny and restrictions on cross-border transfers. As a result, the concept of Important Data has become a central concern in discussions of data governance and corporate compliance in China.

### *Extraterritorial Jurisdiction and the U.S. CLOUD Act*

In contrast to China's sovereignty-based model, U.S. legal scholarship emphasizes the expansion of extraterritorial jurisdiction in data governance. The enactment of the Clarifying Lawful Overseas Use of Data (CLOUD) Act represents a significant shift from a territorial to a control-based approach, enabling U.S. law enforcement agencies to compel disclosure of data held by service providers regardless of its physical location (Swire & Hemmings, 2019). The origins of this shift can be traced to the Microsoft Ireland case, which exposed limitations in existing legal frameworks governing cross-border data access (Kerr, 2018). In response, the CLOUD Act established that jurisdiction depends on whether a company has "possession, custody, or control" over the data, rather than where the data is stored. This interpretation significantly broadens the reach of U.S. law enforcement authority (Murphy, 2020). Scholars have noted that this extraterritorial approach creates inherent tension with foreign data protection laws, particularly those based on territorial sovereignty. While mechanisms such as executive agreements and the motion-to-quash provision exist, their practical effectiveness remains limited, especially in jurisdictions without bilateral agreements with the United States (DOJ, 2021). This structural limitation intensifies conflicts with regulatory systems such as China's DSL and PIPL.

### *Trade Secrets and the Gap in Existing Literature*

Despite extensive academic attention to personal data protection and privacy regulation, relatively limited research has focused on non-personal data, particularly trade secrets, in the context of cross-border data governance. Trade secrets including proprietary algorithms, source code, and R&D data constitute critical assets in the digital economy but are increasingly subject to regulatory frameworks designed primarily for data security and sovereignty. Recent studies suggest that the classification of such information as "Important Data" within China's legal framework significantly increases compliance risks for multinational corporations (Huang, 2024; McKnight, 2023). At the same time, the extraterritorial reach of the U.S. CLOUD Act exposes this data to foreign legal demands, creating a complex and often conflicting regulatory environment. This gap in the literature highlights the need for a focused analysis of trade secrets as a distinct category of data in cross-border legal conflicts. Accordingly, this paper contributes to existing scholarships by examining how trade secret data is situated within competing regulatory frameworks and by analyzing the resulting legal and compliance challenges faced by multinational corporations.

## METHODOLOGY

This study adopts a qualitative comparative legal research methodology to examine the regulatory frameworks governing cross-border data transfers between the People's Republic of China (PRC) and the United States. The research is grounded in doctrinal legal analysis, focusing on the interpretation and comparison of primary legal sources, including China's Data Security Law (DSL) and Personal Information Protection Law (PIPL), as well as the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act. The comparative approach is employed to identify key differences in legal principles, jurisdictional scope, and enforcement mechanisms between the two systems. In particular, the study contrasts China's sovereignty-based model of data governance with the United States' control-based approach to extraterritorial jurisdiction. This comparison enables the identification of structural inconsistencies and areas of legal conflict, especially in relation to the cross-border transfer of commercially sensitive data.

In addition to doctrinal analysis, the study incorporates case-based reasoning to illustrate the practical implications of these legal frameworks. Reference is made to the Microsoft Ireland case as a foundational example that shaped the development of the CLOUD Act, as well as to hypothetical and industry-based scenarios involving multinational corporations (MNCs) operating across jurisdictions. These examples are used to demonstrate how conflicting legal obligations arise in real-world contexts. The research further applies a conflict-of-laws perspective to evaluate the interaction between domestic legal regimes and their extraterritorial effects. By examining how legal obligations overlap and contradict across jurisdictions, the study highlights the emergence of a "Legal Catch-22" in which compliance with one system results in violation of another. This methodological framework allows for a comprehensive assessment of the legal risks faced by multinational corporations handling trade secret data in cross-border environments. It also provides a basis for evaluating the effectiveness of existing compliance strategies and identifying potential pathways for regulatory coordination in the evolving landscape of global data governance.

## RESULTS AND ANALYSIS

This section presents a comparative analysis of the Chinese and United States legal frameworks governing cross-border data transfers. It examines how the interaction between these systems creates structural conflicts, particularly in relation to trade secret data. The analysis is organized into four parts: China's data sovereignty framework, the extraterritorial reach of the U.S. CLOUD Act, the resulting Legal Catch-22, and the implications for multinational corporations.

### *China's Data Sovereignty Framework*

China's data governance system is grounded in the principle of data sovereignty, which treats data generated or stored within its territory as a strategic national resource subject to state control. This approach is institutionalized through the Data Security Law (DSL) and the Personal Information Protection Law (PIPL), which together establish a comprehensive regulatory framework governing the collection, processing, and transfer of data. A central feature of the DSL is its classification system, which categorizes data based on its importance to national security, economic stability, and public interests. Among these categories, "Important Data" represents a critical regulatory concept. Although not exhaustively defined, it broadly includes data that, if disclosed or misused, could affect national interests. In practice, this may encompass commercially sensitive information such as trade secrets, proprietary algorithms, and research and development (R&D) data, particularly in strategic industries. The regulatory framework imposes strict controls on cross-border data transfers. Organizations handling Important Data are required to undergo security assessments and comply with regulatory approval procedures before transferring such data. Article 36 of the DSL serves as a key enforcement mechanism, explicitly prohibiting the disclosure of domestically stored data to foreign judicial or law enforcement authorities without prior approval from competent Chinese authorities. This provision effectively functions as a blocking statute, reinforcing the territorial control of data. The Cyberspace Administration of China (CAC) plays a central role in implementing these requirements, exercising broad authority over data classification, security reviews, and cross-border transfers. The discretionary nature of this regulatory regime, combined with the lack of precise definitions, creates a compliance

environment characterized by uncertainty. Multinational corporations must therefore adopt a cautious approach, often treating a wide range of data as potentially regulated to avoid legal exposure.

### *The U.S. CLOUD Act and Extraterritorial Reach*

In contrast to China's territorially grounded framework, the United States adopts a control-based approach to jurisdiction over data. The Clarifying Lawful Overseas Use of Data (CLOUD) Act extends the authority of U.S. law enforcement agencies by requiring service providers subject to U.S. jurisdiction to disclose data within their "possession, custody, or control," regardless of where the data is physically located. This approach emerged in response to the Microsoft Ireland case, which highlighted the limitations of territorial jurisdiction in an era of cloud computing. By shifting the focus from location to control, the CLOUD Act enables U.S. authorities to access data stored in foreign jurisdictions, including China, provided that the data is accessible by a U.S.-based entity. The Act also introduces mechanisms such as executive agreements, which allow for cross-border data sharing between the United States and partner countries. However, no such agreement exists between the United States and China, leaving a significant gap in legal coordination. While the Act includes a motion-to-quash provision, allowing companies to challenge data disclosure orders under certain conditions, its applicability is limited in practice, particularly in the absence of reciprocal legal arrangements. As a result, multinational corporations operating in China but subject to U.S. jurisdiction face a legal obligation to comply with CLOUD Act orders, even when such compliance may conflict with local laws. This extraterritorial reach significantly expands the scope of U.S. enforcement authority and creates direct tension with sovereignty-based regulatory systems.

### *The Sino–US Legal Catch-22*

The interaction between China's data sovereignty framework and the U.S. CLOUD Act creates a structural legal conflict that places multinational corporations in an untenable position. The core issue lies in the incompatibility between China's territorial restrictions on data transfer and the United States' assertion of extraterritorial jurisdiction based on control. Under the DSL, companies are prohibited from transferring Important Data to foreign authorities without government approval. At the same time, the CLOUD Act mandates compliance with lawful U.S. data access requests, regardless of where the data is stored. This creates a direct conflict of legal obligations: compliance with one regime necessarily results in violation of the other. This situation can be characterized as a "Legal Catch-22," in which companies must choose between breaching Chinese law or facing penalties under U.S. law. The risks associated with this dilemma include financial sanctions, criminal liability, and reputational damage, as well as potential restrictions on market access in either jurisdiction. Practical scenarios illustrate the severity of this conflict. For example, a U.S.-based technology company operating cloud services in China may be required to disclose data stored on Chinese servers in response to a CLOUD Act order. However, doing so without Chinese government approval would violate Article 36 of the DSL. Conversely, refusal to comply with the U.S. order may result in legal penalties in the United States. The absence of effective conflict-resolution mechanisms further exacerbates the problem. Existing legal tools, such as mutual legal assistance treaties, are often too slow or limited to address the immediacy of

digital data access requests. As a result, corporations are left to navigate conflicting legal systems without clear guidance, increasing the overall risk and complexity of cross-border operations.

### *Corporate and Policy Implications*

In response to these legal conflicts, multinational corporations have adopted a range of compliance strategies aimed at mitigating risk. One of the most prominent approaches is data localization, whereby sensitive data is stored and processed within the jurisdiction where it is generated. While this reduces exposure to foreign legal demands, it also increases operational costs and limits the efficiency of global data integration. Another strategy involves encryption-based geofencing, which restricts access to data based on geographic location and organizational control. By limiting the ability of foreign entities to access certain datasets, companies attempt to reduce the applicability of extraterritorial legal claims. However, such measures are not foolproof and may still be challenged under broad interpretations of "control." Organizational restructuring is also used to separate legal entities across jurisdictions, thereby reducing the likelihood that a single entity will be subject to conflicting legal obligations. While effective to some extent, this approach introduces additional complexity in corporate governance and may not fully eliminate legal risk. At the policy level, the lack of coordination between national legal systems remains a critical issue. Existing frameworks, such as Mutual Legal Assistance Treaties (MLATs), are insufficient to address the speed and scale of modern data flows. The absence of a bilateral agreement between the United States and China further intensifies the conflict, leaving a regulatory gap that directly impacts multinational operations. These findings highlight the need for international cooperation and the development of harmonized legal standards for cross-border data governance. Without such efforts, the fragmentation of regulatory regimes is likely to continue, posing ongoing challenges for corporations and policymakers alike.

## CONCLUSION

This paper has examined the growing legal conflict surrounding cross-border data transfers between the People's Republic of China and the United States, with particular focus on the treatment of corporate trade secrets as a category of sensitive data. Through a comparative analysis of China's Data Security Law (DSL) and Personal Information Protection Law (PIPL) and the U.S. CLOUD Act, the study has demonstrated that these regulatory frameworks are built upon fundamentally different legal principles. While China emphasizes data sovereignty and territorial control, the United States adopts an extraterritorial approach based on the concept of possession, custody, or control. The findings reveal that this divergence creates a structural incompatibility that cannot be reconciled under current legal mechanisms. Multinational corporations operating across these jurisdictions are placed in a "Legal Catch-22," where compliance with one legal system necessarily results in violation of the other. In particular, the classification of trade secrets as "Important Data" within China's regulatory framework significantly expands the scope of restriction, while the CLOUD Act's broad disclosure requirements increase exposure to foreign legal demands.

The analysis further highlights that existing compliance strategies—such as data localization, encryption-based geofencing, and organizational restructuring—provide only partial

and temporary solutions. While these measures may reduce immediate legal risk, they do not resolve the underlying conflict between sovereignty-based and control-based models of data governance. As a result, corporations continue to operate in an environment of legal uncertainty, facing potential financial penalties, regulatory sanctions, and operational disruptions. At a broader level, this conflict reflects a deeper fragmentation in global data governance. The absence of effective bilateral agreements or multilateral frameworks between major jurisdictions, particularly between the United States and China, exacerbates the problem and limits the ability of existing mechanisms to address cross-border data access in a timely and coherent manner.

In light of these challenges, the paper underscores the need for greater international cooperation in developing harmonized legal standards for cross-border data transfers. This may include the negotiation of bilateral agreements, the modernization of mutual legal assistance frameworks, and the establishment of global norms that balance national security concerns with the economic necessity of data mobility. As data continues to function as a core driver of innovation and economic growth, resolving these regulatory conflicts will be essential for ensuring the stability and efficiency of the global digital economy. Without such coordination, the increasing fragmentation of legal regimes is likely to impose significant constraints on multinational operations and hinder the development of integrated digital markets.

## REFERENCES

Bonardi, G. (2023). Outbound data transfer from China: Implications for national security and foreign businesses. *SSRN Electronic Journal*.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bygrave, L. A. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Căpușneanu, S., et al. (2025). Reshaping the digital economy with big data: A meta-analysis of trends and technological evolution. *Electronics, 14*(2709).

Chen, X., Zhang, L., & Cheng, X. (2024). Fiscal decentralization and the development of the digital economy: Evidence from China. *Journal of Economic Policy Reform, 27*(3), 276–294.

Colangelo, G. (2025). The privacy/antitrust curse: Insights from GDPR application in competition law proceedings. *Antitrust Bulletin, 70*(1), 113–132.

Daskal, J. (2018). Privacy and security across borders. *Yale Law Journal Forum, 128*, 1029–1049.

Dzigal, N., et al. (2025). *Digital sovereignty and geopolitics in the field of data protection: A comparison of the EU, China, and the USA* [Unpublished manuscript].

Erie, M. S., & Streinz, T. (2021). The Beijing effect: China's Digital Silk Road as transnational data governance. *New York University Journal of International Law and Politics, 54*(1), 1–92.

European Commission. (2022). *The Digital Markets Act: Ensuring fair and open digital markets*.

Galbraith, J. (2018). Congress enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, reshaping US law governing cross-border access to data. *American Journal of International Law, 112*(3), 487–492.

Giladi Shtub, T., & Gal, M. S. (2022). The competitive effects of China's legal data regime. *Journal of Competition Law & Economics, 18*(4), 936–968.

Hongqiang, Z., et al. (2025). Data compliance in cross-border e-commerce: A comparative study of China and Malaysia's regulatory frameworks. *Global Academic Frontiers, 3*, 65–78.

Hug, F. (2024). Rules governing state-owned enterprises: Competition, coordination, and control. In *China's Free Trade Agreement Strategies* (pp. 139–165). Springer.

Khan, J., & Belk, R. (2024). Case study two: China's e-CNY or digital RMB. In *Digital Currency and Consumption* (pp. 261–280).

Li, Q. (2025). Excessive data collection and (mis) use of data: A comparative law and economics study on the Chinese Didi case and the German Facebook case. *Chinese Journal of Comparative Law, 13*, Article cxae018.

Li, W. C. Y., Nirei, M., & Yamana, K. (2019). *Value of data: There's no such thing as a free lunch in the digital economy*. Research Institute of Economy, Trade and Industry (RIETI).

Li, Z., et al. (2025). Impact of the General Data Protection Regulation on the global mobile app market: Digital trade implications of data protection and privacy regulations. *Information Systems Research, 36*, 669–685.

Lin, X. (2025). A model of big data-based governance: China's national government big data platform and an analysis of its governance competence. *Chinese Political Science Review*, 1–22.

Mulligan, S. P. (2018). *Cross-border data sharing under the CLOUD Act* (CRS Report No. LSB10135). Congressional Research Service.

Nettesheim, M. (2023). Data protection in contractual relationships (Art. 6 (1)(b) GDPR). *SSRN Electronic Journal*.

Roccon, M. (2023). *Foreign investment in China's cloud industry: A case study of Microsoft Azure's expansion* [Unpublished manuscript].

Rughiniș, R., et al. (2021). From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. *Computer Law & Security Review, 42*, 105585.

Schwartz, P. M. (2018). Legal access to the global cloud. *Columbia Law Review, 118*(6), 1681–1762.

Seuwou, P. (2025). *Digital business: Navigating the digital landscape and thriving in the digital economy*.

Shao, D., et al. (2025). Comparative analysis of data protection regulations in East African countries. *Digital Policy, Regulation and Governance, 27*, 486–505.

Shen, Y., & Zhang, B. (2025). Advancing the emergency industry: Policy, innovation, and implications for national security. *Journal of the Knowledge Economy, 16*, 6907–6925.

Shi, Y., & Wei, F. (2025). Comparative analysis of digital economy-driven innovation development in China: An international perspective. *Journal of the Knowledge Economy, 16*, 4422–4445.

Shukla, S., et al. (2023). *Data economy in the digital age*.

Shurson, J. (2023). *Rethinking comity: Resolving conflicts in transnational digital investigations* [Doctoral dissertation, Queen Mary University of London].

Sitompul, J. (2020). *Cross-border access to electronic evidence: Improving Indonesian law and practice in investigating cybercrime*.

Streinz, T. (2021). The evolution of European data law. In P. Craig & G. de Búrca (Eds.), *The Evolution of EU Law* (3rd ed., pp. 902–936). Oxford University Press.

Suntsova, O. (2024). Digital transformation of the global economy: Challenges and opportunities. *SSRN Electronic Journal*.

Vandendriessche, R., & Buts, C. (2025). Separating or integrating? Data protection in competition assessments: A systematic literature review. *European Competition Journal*, 1–30.

Voss, W. G., & Pernot-Leplay, E. (2024). China data flows and power in the era of Chinese big tech. *Northwestern Journal of International Law & Business, 44*(1), 1–55.

Wang, C. C., Liu, U., & Dong, H. H. (2025). The United States' strengthened national security review of Chinese investment: Implications from the tech war. *American University International Law Review, 40*, 1151–1180.

Wang, X., & Huang, Y. (2022). China's antimonopoly law enforcement in the digital economy. *Antitrust Bulletin, 67*(4), 562–578.

Xu, W., & Kievich, A. V. (2024). The main trends in the digital economy and finance that shape the current landscape and vector of development of industries. *Economy & Banks*, 42–55.

Yu, Y. (2023). *The interaction between competition (law) and data protection (law) for privacy protection in digital markets* [Unpublished manuscript].

Yun, H. (2025). China's data sovereignty and security: Implications for global digital borders and governance. *Chinese Political Science Review, 10*, 178–199.