Data Governance Policy Analysis from an International Perspective: Development Situation and Policy Recommendations

Authors: Li Chengxi, Wu Xinnian, Wu Xinnian

Date: 2023-04-11T00:00:00+00:00

Abstract

Purpose/Significance Strengthening global data governance has become a contemporary international strategic consensus, while data sovereignty has emerged as a critical manifestation of national sovereignty in cyberspace. Numerous countries worldwide are actively formulating data governance policies and engaging in global data governance competition. Consequently, researching and analyzing the data governance policies and practices of developed nations holds significant importance for the construction of China's data governance system and capabilities.

Methods/Process Through comparative analysis of data governance policies and practices enacted by the United States, the European Union, and Japan, this study clarifies the core content, value orientations, and practical pathways of these regions' data governance policies, assesses the development trends in global data governance, identifies the primary challenges currently confronting China's data governance, and proposes strategic recommendations for strengthening China's data governance system and capacity building.

Results/Conclusion To effectively enhance China's data governance capacity, it is imperative to improve the institutional and legal frameworks for data governance, maintain a focus on international competition, seize discourse power and rule-making authority in global data governance competition, actively construct an open and collaborative data governance cooperation pattern, continuously refine data governance operational mechanisms, and promote the opening of public data and the optimization of governance technologies in China.

Full Text

Data Governance Policy Analysis from an International Perspective: Development Trends and Strategic Recommendations

LI Chengxi[1],[2], **WU Xinnian**[1],[2]
[1] Northwest Institute of Eco-Environment and Resources, Chinese Academy of Sciences, Lanzhou 730000
[2] School of Economics and Management, University of Chinese Academy of Sciences, Beijing 100049

Abstract

[**Purpose/Significance**] Strengthening global data governance has emerged as an international strategic consensus, with data sovereignty representing a critical extension of national sovereignty into cyberspace. Numerous countries have actively formulated data governance policies and engaged in global competition for data governance leadership. Consequently, examining and analyzing the data governance policies and practices of developed nations holds significant importance for China's data governance system development and capacity building. [**Method/Process**] This study conducts a comparative analysis of data governance policies and practices from the United States, European Union, and Japan to clarify their core content, value orientations, and implementation pathways. It assesses global data governance trends, identifies key challenges facing China's data governance, and proposes strategic recommendations for strengthening China's data governance system and capabilities. [**Result/Conclusion**] To effectively enhance China's data governance capacity, the nation should improve its institutional and legal frameworks for data governance, focus on international competition to secure discourse power and rule-making authority in global data governance, actively construct an open and cooperative data governance architecture, continuously refine operational mechanisms, and promote public data opening while optimizing governance technologies.

Keywords: Global Governance; Data Governance; Data Sovereignty; Data Opening; Data Monopoly

In the digital economy era, data is regarded as one of the most important factors of production and a new driver of socio-economic operation. However, frequent global incidents of data breaches, tampering, and misuse in recent years have gradually exposed deficiencies in data governance. As artificial intelligence technologies achieve continuous performance breakthroughs, generative AI systems like ChatGPT are revolutionizing human knowledge production, accompanied by thorny issues concerning data quality, privacy, and technical vulnerabilities hidden behind these systems. Countries worldwide face a series of data security and national security challenges, while data sovereignty, as a crucial component of national sovereignty, concerns national interests and security. Actively for-

mulating and improving data governance policies to promote data openness and sharing, realize data value conversion, and safeguard data sovereignty has become the focus of a new round of great power competition. In light of this, this paper analyzes the data governance policies and practices of the United States, European Union, and Japan, summarizing their policy motivations and characteristics to provide reference and lessons for China's data governance system and capacity building.

1.1 United States: From Government Data Opening to Global Data Competition

U.S. data governance policy has generally evolved through three stages, with policies in different periods being both continuous and distinctively focused. **First, the Obama Administration (January 2009–January 2017):** This era prioritized government information transparency and the construction of a new data governance framework. Building on traditions emphasizing freedom of information, the Obama Administration strengthened information mining and utilization in 2009, promoted IT transformation, and focused on using information to upgrade traditional industries while advancing the information industry. Consequently, in its first year, the administration issued two key policies—the *Memorandum on Transparency and Open Government* and the *Open Government Directive*—to promote U.S. government information disclosure, explicitly proposing "to build an unprecedentedly open government" with the goal of ensuring all information operates in the sunshine. In March 2012, the Obama Administration promulgated the *Big Data Research and Development Initiative*, America's first national strategy centered on big data R&D, which opened the prelude to global big data strategic competition. In May 2012, it issued the *Digital Government: Building a 21st Century Platform to Better Serve the American People* strategy, aiming to foster a new type of digital government oriented toward public services and adopting a "small government–big society" model of joint national and social governance, establishing a solid foundation for U.S. data governance.

As U.S. data openness continued to increase, the government gradually recognized the importance of data resources as assets. Consequently, policies such as the *Open Data Policy—Managing Information as an Asset*, *Open Government Partnership—U.S. Second Open Government National Action Plan*, and *Making Open and Machine Readable the New Default for Government Information* emphasized the importance of treating government data as critical assets for actual operation and improving data management efficiency. In May 2016, the U.S. government released the *Federal Big Data Research and Development Strategic Plan*, proposing seven data development strategies covering big data technology R&D, data sharing, data quality, data infrastructure, privacy security, talent cultivation, and enhanced cooperation, aiming to build a vibrant national big data innovation ecosystem.

Second, the Trump Administration (January 2017–January 2021):

This period continued promoting government data opening while vigorously controlling external data competition. During the 2016 presidential campaign, Trump repeatedly emphasized his firm stance as an "America First" advocate, making this principle a key concept in his administration's data governance approach. In March 2018, the U.S. enacted the *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), granting the government law enforcement authority to access data stored overseas by domestic companies. In June 2018, the National Institutes of Health released the *Strategic Plan for Data Science* to store, manage, standardize, and publicly disclose massive biomedical research data. In December 2018, Trump signed the *Open Government Data Act*, elevating U.S. open government data to the legal level and providing legal guarantees for government data opening and utilization. In December 2019, the White House Office of Management and Budget released the *Federal Data Strategy 2020 Action Plan* to guide federal agencies in strengthening data governance, using data to accomplish missions, serve the public, and manage resources while respecting privacy and confidentiality.

Moreover, the Trump Administration demonstrated high sensitivity externally, such as banning TikTok under the pretext of "protecting national data security." This approach resembled political behavior more than data protection governance, aiming to aggressively suppress competitive Chinese enterprises in the United States. On December 22, 2020, the Department of Homeland Security released the *Data Security Business Advisory—Risks and Considerations for Businesses Using Data Services and Equipment from Companies with Chinese Connections*, a warning to U.S. businesses about data security risks that recommended "replacing Chinese data service providers and equipment." This represented the extreme manifestation of U.S. unilateralism and protectionism.

Third, the Biden Administration (January 2021–present): This era has placed greater emphasis on national cybersecurity and strengthening global data competition dominance. After taking office, the Biden Administration not only continued the Trump Administration's restrictions and suppression of Chinese enterprises under the pretext of data security but also made cybersecurity and global data competition strategic priorities. In April 2021, the Office of the Director of National Intelligence released the *2021 Annual Threat Assessment Report*, which emphasized cybersecurity issues and identified Russia, China, Iran, and North Korea as primary U.S. adversaries in international competition. Subsequently, the Biden Administration issued the *Executive Order on Improving the Nation's Cybersecurity* and *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries* to strengthen the U.S. cybersecurity control system. In cross-border data flows, the Biden Administration promoted the "Indo-Pacific Economic Framework" and "Trans-Atlantic Data Privacy Framework," gradually revealing a U.S.-EU collaborative model for cross-border data governance dominance.

As early as May 2020, the U.S. Agency for International Development released America's first digital cooperation policy document—the *Digital Strategy (2020–*

2024)—which declared that the U.S. would continue its "global leadership" role in the digital domain and "not leave developing countries behind or marginalized." This marked the formal launch of U.S. digital cooperation based on American values, making international digital cooperation a central issue in Biden's foreign policy. However, on the TikTok ownership issue, despite TikTok's attempts to alleviate U.S. concerns through concrete actions like "Project Texas," the Biden Administration still coerced ByteDance to sell its TikTok shares through threats of banning the application. This inconsistency between policy and practice—promising not to marginalize developing countries while unreasonably suppressing Chinese enterprises—demonstrates that the U.S. can no longer dominate global data governance alone, and Biden's advocated international digital cooperation is clearly colored by America First ideology.

On March 31, 2023, the White House Office of Science and Technology Policy officially released the *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics*, establishing government-supported goals for privacy-preserving data sharing and analysis, providing policy guarantees for realizing data value utilization and improving data privacy protection.

In summary, the Obama Administration pioneered U.S. government data opening and sharing pathways, with related policies and practices laying the core foundation for U.S. data governance development. The Trump and Biden Administrations' data governance policies continued Obama's emphasis on data opening and sharing, data quality management, and IT development. The difference lies in that the Trump Administration adhered to the "America First" principle, always prioritizing U.S. interests, while the Biden Administration places greater emphasis on strengthening international cooperation, seeking to consolidate global data competition dominance by uniting allies. However, this international cooperation is actually selective and exclusive. Overall, U.S. data governance policy demonstrates a trajectory of "government data opening and sharing—vigorously controlling external data competition—strengthening global data competition dominance." These three policy directions are not isolated but intertwined and mutually supportive, particularly the U.S. strategic positioning of China as a primary adversary in cybersecurity and data competition, which deserves China's serious attention.

1.2 European Union: Data Sovereignty Maintenance Based on Data Protection Strategy

Data sovereignty internally reflects a state's supreme jurisdiction over data, while externally manifesting as independence, autonomy, and cooperation rights in cyberspace data. Compared with the U.S. proactive, offensive data governance policies and practices, the EU has formed a defensive strategy for strengthening data sovereignty based on data protection. In 1995, the EU adopted the *Directive on the Protection of Personal Data* (hereinafter "the Directive"), which employed a unified legislative model, stipulated the establishment of independent data protection authorities, and offered relatively strong protection for

data subjects' rights but somewhat damaged data circulation efficiency. To optimize and compensate for the Directive's deficiencies, the European Parliament passed the *General Data Protection Regulation* (GDPR) in April 2016. Based on human rights values, GDPR, as an EU regulation, grants data subjects more rights and equips data protection supervisory authorities with diversified enforcement tools. Together with the *Regulation on the Free Flow of Non-Personal Data* jointly promulgated by the European Parliament and the Council of the EU in November 2018, GDPR promotes the free flow and extensive use of data within the EU while vigorously fostering EU data economy development through high-level privacy protection mechanisms, data security measures, and ethical standards.

The "Digital Single Market" serves as an important means for the EU to achieve its data protection strategy, with its core connotation being strict data protection for EU member states. In May 2015, the EU released the *Digital Single Market Strategy for Europe*, aiming to establish a new, unified digital market to promote digital economic development among EU member states while achieving data protection. In 2017 and 2018, the EU successively issued *Building a European Data Economy* and *Towards a Common European Data Space*, attempting to establish a core digital market across Europe to promote data opening and sharing and data economic development among EU countries, intending to use the "Digital Single Market" to exercise jurisdiction over data subjects. In February 2020, the EU's *European Data Strategy* raised the banner of digital economy development and laid out a vision to make Europe the world's most attractive, safest, and most dynamic data-agile economy by 2030. In March 2021, the EU released *2030 Digital Compass: The European Way for the Digital Decade*, proposing 12 digitalization goals to reduce EU dependence on foreign technologies and defend EU digital sovereignty. In May 2022, the EU formally enacted the *Data Governance Act*, whose concepts of "data altruism" and "data intermediaries" will further advance the EU's strategic vision of establishing a "Digital Single Market." In November 2022, the *Digital Markets Act* and *Digital Services Act* officially took effect, providing more solid legal guarantees for EU digital market innovation, clear responsibilities, and transparent environments.

2.1 Consistent Policy Core Content: Focusing on Data Opening and Data Security

Public data opening represents an inevitable trend in modern economic and technological innovation development, as the mining and utilization of data as a factor of production has become a key determinant of future competitiveness. Countries worldwide have recognized that opening public data is one of the necessary conditions for digital economy development and an important task of data governance. The issuance of policies such as the U.S. *Memorandum on Transparency and Open Government*, *Open Government Directive*, and *Open Government Data Act*, the EU's GDPR, and Japan's *Open Data 2.0* and *Open Data Basic Guidelines* not only guarantees citizens' right to information freedom

but also provides strong policy and legal support for opening government data. However, the process of data opening and sharing can trigger data security issues at both personal and national levels, requiring state agencies to proactively identify problems and formulate data security governance policies to ensure data security and even national security. Consequently, the U.S. *CLOUD Act* and *Department of Defense Data Strategy*, the EU's *European Digital Sovereignty* and *Data Governance Act*, and Japan's *Basic Act on Cybersecurity* and *Basic Act on the Formation of a Digital Society* have all actively explored data security governance pathways. In summary, the data governance policies of the three major economies—the U.S., EU, and Japan—show considerable similarity in core content, all focusing on promoting data opening and sharing while maintaining national data security.

2.2 Consistent Policy Value Orientation: Competing for Data Governance Dominance

Driven by pressure from global data governance competition, the U.S., EU, and Japan all pursue the deep value orientation of seizing dominance in global data governance competition to enhance their competitive positions. The U.S. *Digital Cooperation Strategy (2020–2024)* explicitly states that America should continue to play a "global leadership" role in the digital domain. The *U.S. Innovation and Competition Act of 2021*, passed by the U.S. Senate in June 2021, contains 67 sections addressing competition with China in the digital economy, focusing on key areas such as digital technology, digital security, and digital rules, marking a comprehensive, systematic legal effort to contain China's digital development. The EU, through policies like GDPR and the *Digital Single Market Strategy*, competes for global data governance dominance, while the *Digital Services Act* and *Digital Markets Act* aim not only to strengthen domestic data governance leadership but also to extend EU legal systems globally, enhancing EU discourse power and rule-making authority in global data governance. Japan's *U.S.-Japan Digital Trade Agreement*, *Osaka Declaration on Digital Economy* signed with G20 members, and its leadership in CPTPP multilateral negotiations represent active efforts to seize global data governance dominance.

2.3 Divergent Governance Practices: Optimal Paths Based on National Conditions

Although the U.S., EU, and Japan share considerable consistency in policy core content and value orientation, their specific data governance policy practices differ, as each country adopts different pathways based on its national conditions and developmental advantages in data governance.

2.3.1 United States: Data Hegemonism Under Double Standards

The U.S. practices double standards in global data governance issues. On one hand, it promotes data free flow and open sharing through policy documents,

calling on other countries to facilitate data free flow. On the other hand, it enacts strict data protection policies like the *CLOUD Act* to expand its judicial jurisdiction over data, eliminate obstacles to obtaining extraterritorial data, and strictly protect U.S. data. Additionally, the U.S. enacted the *Foreign Intelligence Surveillance Act* to extend digital surveillance globally, conducting large-scale data collection and theft. Overall, the U.S. unilaterally emphasizes free flow of other countries' data while adopting strict protection measures for its own data. Its "indiscriminate" surveillance of both competitors and allies contradicts Biden's executive order "prohibiting government use of commercial spyware." Ultimately, the U.S. can implement double standards due to its powerful economic and technological strength, and this data hegemonism under double standards represents the politicization of data governance, posing threats and obstacles to global data governance development.

2.3.2 European Union: Expanding Legislative Jurisdiction to Influence Global Data Legislation

The EU's GDPR demonstrates its legislative intent to actively expand the scope of EU law application. GDPR Articles 3(1) and 3(2) define its territorial scope, proposing "establishment criteria" and "targeting criteria," while Article 3 addresses application based on international law rules. Since GDPR took effect on May 25, 2018, it has generated substantial global influence, prompting other countries to subsequently launch data legislation. For example, Brazil's Senate passed the *Brazilian General Data Protection Law* in July 2018, India's High-Level Committee released the *Personal Data Protection Bill, 2018 (Draft)* in the same month, and even California passed the *California Consumer Privacy Act of 2018* in June 2018. These data laws (drafts) have all drawn on GDPR provisions to varying degrees, demonstrating both the importance of personal data protection in global data governance and increasing the EU's possibility of expanding extraterritorial jurisdiction through data legislation. GDPR has become a blueprint for data policies in the UK, France, Germany, and other countries, and China's *Personal Information Protection Law*, enacted in 2021, also borrowed its extraterritorial jurisdiction provisions. In short, as the world's first comprehensive personal data protection law, GDPR has profoundly influenced data protection legislation processes in Europe and worldwide.

2.3.3 Japan: Using Data Governance Diplomacy to Compete for Discourse Power

Japan's data governance policy practice pathway primarily involves data governance diplomacy through concept promotion and bilateral/multilateral negotiations, as Japan seeks not merely to participate in basic discussions on global data governance but to use critical timing and main advantages to dominate global data governance rule-making. Japan's data governance diplomacy exhibits three main characteristics: First, "proactive proposal"—Japan firmly grasps key opportunities in important occasions to 率先 propose innovative data

governance concepts, leading discussions and formulation of data governance rules. Second, "continuous reinforcement"—Japan continuously strengthens its innovative data governance concepts through persistent concept promotion, bilateral/multilateral negotiations, and agreement signings in important occasions and critical moments, enhancing its global influence and universal concept recognition. Third, "emphasis on cooperation"—Japan actively constructs strategic cooperation with developed countries, efficiently using data governance diplomacy through regional international conference exchanges and international agreement signings to enhance Japan's international discourse power in data governance.

3.1.1 Low Global Influence of Extraterritorial Jurisdiction in Data Legislation

The global game of extraterritorial jurisdiction in data legislation represents an important pathway to safeguarding national data sovereignty. The U.S., based on the value concept of "data free flow," continuously extends its unilateral power to 调取 extraterritorial data, while the EU, based on human rights-oriented data protection concepts, endows GDPR with extraterritorial jurisdiction. China's data legislation developed relatively late. Although both the *Data Security Law* and *Personal Information Protection Law* clearly define application scope and necessary extraterritorial effect, their global influence on extraterritorial jurisdiction remains relatively weak compared with Europe and the U.S. Particularly, provisions addressing cross-border data and data security issues resemble defensive countermeasures under the proactive offensive of European and American countries. The *Cybersecurity Review Measures*, effective February 15, 2022, added data security review provisions to prevent Chinese user data from becoming a tool for other countries to analyze and monitor China. Extraterritorial jurisdiction is a prerequisite for national law's extraterritorial application, and expanding the extraterritorial scope of data legislation constitutes an indispensable factor in competing for global data governance dominance. However, in global data governance competition, the extraterritorial effect of data legislation is influenced by political, economic, legal, and technological factors. Actively participating in and promoting the formation of global data governance standards and rules is key to enhancing the global influence of China's specialized data legislation's extraterritorial jurisdiction.

3.1.2 Insufficient Public Data Opening and Weak Industrial Data Sharing

Open sharing is a prerequisite for developing and utilizing public data value. Compared with the U.S., EU, and Japan, despite China's issuance of policies such as the *Opinions on Improving the Mechanism for Market-oriented Allocation of Production Factors* and the *Outline for Promoting Big Data Development* that explicitly propose promoting government data opening, government public data opening still faces "unwillingness, fear, and inability" issues constrained by

processes, concepts, and management systems. The main differences manifest in three aspects: First, different government data supervision systems—the U.S., EU, and Japan primarily promote public data opening and sharing through legislation, with relatively little specific intervention in public data opening, emphasizing data markets and social freedom. In contrast, due to lagging legislation, Chinese government management departments, considering authority and interests, exhibit resistance and buck-passing toward public data opening, causing relevant data subjects to be unwilling to open data. Second, different degrees of strictness in data security protection—while the U.S., EU, and Japan attach great importance to data security protection, they also highly value data value development and utilization. Chinese governments, however, fear data leaks from data opening, worry about data quality issues becoming prominent after opening, and face strict administrative regulations and procedures for public data use, resulting in low data utilization efficiency. Third, different core data governance technologies—the U.S., EU, and Japan leverage IT advantages to empower public data opening with relatively small technical obstacles, while some Chinese data subjects lack the technical capacity to participate in data opening, creating another major obstacle. Additionally, although the Chinese government has issued multiple policy documents encouraging industrial data sharing, such as the *Notice of the General Office of the State Council on Issuing the Action Plan for Promoting Big Data Development* and the *Notice of the National Development and Reform Commission and Ministry of Industry and Information Technology on Issuing the 13th Five-Year Plan for Informatization*, which clarified basic principles and requirements for data sharing and provided legal basis and guidance for enterprises, the lack of unified data sharing standards and interest balancing mechanisms among enterprises leads to low sharing willingness. Moreover, different enterprises use different data governance technologies, resulting in poor interoperability and difficulties in industrial data sharing.

3.1.3 Data Monopoly Crisis and Antitrust Challenges

Due to the scale effects of data acquisition and their ability to strengthen corporate dominance, some enterprises can achieve data volume monopolies using technological and infrastructure advantages, transforming data resources into data assets with market competitive advantages, forming profit-oriented active data monopolies. This differs from passive data monopolies of public data resources due to government "unwillingness, fear, and inability." With social digital development, massive data stored by large technology companies poses increasingly significant threats to national economic and data security. U.S. companies like Google, Facebook, Twitter, and Amazon use data to improve products and services, thereby occupying most market share and forming data monopolies driven by profit. Such data monopolies can lead not only to data leaks, privacy violations, and data misuse but also political issues. For example, during the 2016 U.S. presidential election, Facebook was embroiled in a scandal over manipulating the election and was ultimately confirmed to have data leak

problems. Similarly, China's four internet giants—Baidu, Alibaba, Tencent, and JD.com (BATJ)—also possess vast amounts of user, supplier, and transaction data. To better promote industrial data opening and sharing and protect user data security, BATJ should learn from the U.S. experience to avoid risks of data misuse and leaks caused by data monopolies. In summary, data-based monopolies are gradually becoming an important means for internet enterprises and some developed countries to maintain global data competition status, drive out competitors, and contain other countries' economic development. Therefore, in the global data governance competition landscape, antitrust has become one of the important issues in data governance. However, China still faces obvious obstacles in addressing antitrust: First, intense global data competition restricts multinational enterprise development, as Western countries led by the U.S. use IT advantages and diplomatic influence to establish data hegemony and intentionally form data monopolies, threatening China's data sovereignty and national security. Second, the legal system is imperfect with weak regulation and enforcement. Although China has issued a series of antitrust regulations including the *Anti-Monopoly Law* and *E-Commerce Law*, these regulations' application scope and standards remain somewhat ambiguous, resulting in difficult enforcement and weak effectiveness.

3.1.4 Constraints from Core Technologies and Computing Costs

First, data governance requires substantial computing resources and high-end technical means to implement. Processes such as data mining, storage, and analysis necessitate large-scale data centers, databases, and graphics cards. However, Chinese technology companies still lag behind foreign tech giants in these areas, with many core data governance technologies and tools relying on foreign open-source products. Second, China faces bottlenecks in chip manufacturing and high-performance computing. Due to historical reasons and insufficient technological accumulation, China's semiconductor manufacturing technology lags behind international advanced levels, limiting China's development in high-performance computing. Particularly in recent years, the U.S. has besieged China's chip industry by blocking chip production and supply and restricting normal economic and trade activities of chip-related enterprises in China. In 2022, the Biden Administration signed the *CHIPS and Science Act* to strengthen U.S. chip technology leadership, continuing to suppress and interfere with global chip industry development with "America First" values. In summary, data sharing among Chinese government, enterprises, and research institutions remains constrained by algorithm costs and technical standards, as different organizations use inconsistent information systems and data processing standards, increasing data sharing difficulty and reducing willingness for open sharing. Small and medium-sized enterprises particularly cannot afford the costs of building large computing platforms, and China's high electricity costs further increase energy consumption expenses for computing equipment. Additionally, China's data volume grows exponentially, far exceeding the pro-

cessing capacity limits of individual data subjects. Computing cost issues may cause some subjects to choose low-quality algorithms, ultimately affecting data accuracy and reliability, forming a constraint on improving China's data governance capabilities.

3.2.1 Improving Institutions and Legal Frameworks

In February 2023, the CPC Central Committee and State Council issued the *Overall Layout Plan for Digital China Construction* (hereinafter "Digital China Plan"), which proposed optimizing the domestic environment for digital development and strengthening organizational leadership and institutional mechanisms. Meanwhile, the Second Plenary Session of the 20th CPC Central Committee adopted the *Plan for Reforming Party and State Institutions*, proposing to establish the National Data Bureau, echoing the Digital China Plan. As a national agency coordinating digital economy planning and development, the National Data Bureau's establishment represents an important manifestation of adapting to digital economy era development requirements and promoting China's digital strategic transformation. To achieve efficient data governance, China should use the National Data Bureau as the leadership core to construct a downward-extending and compatible data governance system, establish data governance agencies at different levels, clarify agency functions and division of labor, and build and improve multi-party coordination mechanisms. Various data subject agencies and departments should maintain close connections and mutual support, forming an integrated network for China's data governance.

In recent years, China's data governance legal construction has developed rapidly, with laws and regulations such as the *Data Security Law*, *Personal Information Protection Law*, and *Measures for Security Assessment of Cross-border Data Transfer* issued successively since 2021. However, these legal systems have different focuses, and strengthening China's data governance and promoting data industry development requires higher-level institutional construction and legislative design. For example, targeted specialized data legislation is needed to address issues such as cross-border data, data rights confirmation, and data transactions in data governance development. On February 25, 2019, General Secretary Xi Jinping first proposed at the second meeting of the Central Committee for Comprehensively Governing the Country According to Law to "accelerate the construction of China's legal system for extraterritorial application," providing important guidance. Stipulating laws' extraterritorial effect and implementing blocking statutes are common international practices for handling jurisdiction conflicts, which can maintain China's interests to a certain extent under the principle of reciprocity. Therefore, China should base itself on national realities, under the leadership of core state agencies, adhere to the overall national security concept, improve the domestic specialized data legal system, especially accelerate the strategic layout of foreign-related rule of law construction for data, and actively influence, participate in, and even lead the formation of unified international data

governance rules.

3.2.2 Focusing on International Competition to Seize Discourse Power and Rule-Making Authority

International competition has entered the stage of cyber politics, with increasingly fierce global competition surrounding data resources, data governance rules, and discourse power. All countries recognize data's fundamental and strategic position as a factor of production in digital economy development, thus making the seizure of data resource monopolies and international data governance rule-making power a national-level strategy for digital economy development. Japan has strengthened its international discourse power and rule-making authority in global cross-border data flow governance by actively promoting the DFFT concept and participating in bilateral/multilateral negotiations. The EU's GDPR has become a blueprint for extraterritorial jurisdiction legal systems not only in the UK but also in India, Brazil, South Africa, Australia, and other countries, with China also borrowing its Article 3 provisions to create extraterritorial jurisdiction in its *Personal Information Protection Law*. Due to conflicts in data governance concepts among countries, exporting national data governance concepts and values and seizing global data governance discourse power is particularly important in global data competition. The stronger the persuasiveness, influence, and authority-building capacity of data discourse power, the easier it is to gain trust, which benefits occupying an important position in global data governance competition. Compared with U.S. and European technological advantages and rule dominance, emerging countries as "late entrants" need to rely more on international law to safeguard their interests, and "data sovereignty" precisely provides them with powerful theoretical support. Therefore, China should actively use platforms and channels such as APEC, the WTO, the Belt and Road Initiative, BRICS, and the Boao Forum for Asia to export data governance propositions, safeguard China's data sovereignty, thereby enhancing China's discourse power in global data governance, expanding the extraterritorial effect of China's data legislation, promoting China's rule-leading capacity in global data governance, and expanding regional/global data governance rule-making authority.

3.2.3 Emphasizing International Cooperation to Build an Open and Win-Win Data Governance Cooperation Framework

With IT development, countries' interdependence continues to deepen, and global data governance keeps advancing. Data governance is no longer a single country's affair, as nations worldwide attempt to seek data governance cooperation through regional international organizations because cooperation with allies helps establish long-term mechanisms for containing strategic adversaries in the digital age. Meanwhile, as the world's second-largest economy and the

initiator of the Belt and Road Initiative, China should assume major country responsibilities and commitments, actively promoting global data governance and bridging the digital divide. Therefore, China should more actively participate in bilateral/multilateral negotiations on global data governance under the principles of reciprocity and respect for other countries' data sovereignty and interest appeals, promoting the construction of an open and win-win data governance cooperation framework. As a developing country, China exploring mature data governance regulatory construction experience in the process of regional economic collaborative development is more feasible. China can select countries along the Belt and Road and ASEAN member states that maintain long-term economic exchanges with China as global data governance cooperation partners, condensing the concepts of a community with a shared future for mankind and a community with a shared future in cyberspace into global data governance consensus, using group values to enhance mutual trust and cooperation among nations, strengthening countries' trust and support for China, and building a multi-country unified and efficient data governance platform based on trust mechanisms. Meanwhile, global data governance requires reasonably protecting all parties' interests and meeting all parties' development needs, constructing a sound data governance system and legal framework, and enhancing the international influence of China's data legislation's extraterritorial jurisdiction, which not only helps reasonably resolve data jurisdiction disputes but also facilitates building internationally unified judicial adjudication standards.

3.2.4 Improving Operational Mechanisms to Promote Data Opening and Governance Technology Optimization

The 20th CPC National Congress report proposed to "coordinate development and security, and safeguard the new development pattern with a new security pattern." Security is the prerequisite for development, and development is the guarantee of security. For China's data governance, data subjects should continuously improve data governance institutional mechanisms under the premise of ensuring data security, actively promote opening of public data resources and industrial data sharing, to realize data resource value conversion and fully empower China's economic and social development. First, government departments can use public data authorized operation methods to promote government data opening and sharing. Public data authorized operation is an innovative model of government-third party cooperation to mine data value and promote data opening and sharing. However, as this is a completely new data opening and sharing model, public data authorized operation still faces multiple dilemmas in concepts, measurement, norms, and supervision, urgently requiring further exploration and practice. Second, enterprises can build industrial clusters, industrial data alliances, and industrial data sharing pools to establish unified and efficient industrial data sharing rules and standards based on data value and industrial development needs, thereby breaking industrial data sharing barriers and avoiding data monopoly risks. Third, the government can prevent data monopolies or reduce their impact through strengthened market

supervision and encouragement of fair competition, thereby protecting fair competition in domestic data markets. Meanwhile, improving cross-border data flow mechanisms and designing data flow security assessment tools can guard against infringements on China's data sovereignty and national security by foreign data monopolies or data hegemony. Finally, advanced technology is the core support for data governance. Relevant departments should coordinate resources, strengthen IT industry cooperation with countries along the Belt and Road, make up for technological shortcomings in chips and key basic software, leverage the development opportunity of the "East Data West Computing" project to optimize data factor and computing power resource allocation, and use technologies such as blockchain and privacy computing to reduce trust costs in data opening, sharing, and cross-border flow, improve the core data governance technology system, actively promote technological innovation, and break data monopoly barriers.

References

[1] Li Yibin, Liu Yang. Current Status, Challenges, and New Responses of U.S. Data Governance[J]. China Information Security, 2022, 149(04): 75-79.
[2] Cheng Ying. U.S. Releases Federal Data Strategy and 2020 Action Plan[EB/OL].[2023-03-07].http://www.echinagov.com/news/272975.htm.
[3] Jinghua Times. Trump Emphasizes "America First" in Nomination Speech[EB/OL].[2023-03-15]http://m.haiwainet.cn/middle/232591/2016/0723/content_{30120549}1.html.
[4] NIH. NIH releases strategic plan for data science[EB/OL].[2023-03-06].https://www.nih.gov/news-events/news-releases/nih-releases-strategic-plan-data-science.
[5] Hong Weida. Research on Policy Coordination of China's Open Government Data Based on Text Analysis[D]. Heilongjiang University, 2021.
[6] Yang Jing, Kang Qi, Li Zhe. Analysis and Enlightenment of U.S. Federal Data Strategy and 2020 Action Plan[J]. Journal of Intelligence, 2020, 39(09): 150-156+94.
[7] Zuo Xiaodong. Refuting the U.S. Department of Homeland Security's Data Security Business Advisory[EB/OL].[2023-03-11]https://www.secrss.com/articles/28830.
[8] China Youth Daily. U.S. Intelligence Report Again Hypes China as "Top Threat," Becoming "Near-Peer Competitor"[EB/OL].[2023-03-11]https://baijiahao.baidu.com/s?id=1697003856114420055&wfr=spider&for=pc.
[9] Sun Haiyong. U.S. Digital Strategy Toward China: Priorities, Characteristics, and Prospects[J]. Peace and Development, 2022, 189(05): 26-44+140-141.
[10] Cheng Haiye. Biden Administration's Digital Cooperation Strategy: Intentions, Actions, and Limits[J]. World Economics and Politics Forum, 2022, 353(04): 22-43.
[11] Global Times. TikTok Response[EB/OL].[2023-03-16]https://mp.weixin.qq.com/s/*{{{EKptMCx8POuHw}*
[12] GoUpSec. U.S. Releases National Strategy to Advance Privacy-Preserving Data Sharing and Analytics[EB/OL].[2023-04-06] https://www.goupsec.com/news/11841.html.
[13] Zhang Xiaojun. Models and Lessons for Data Sovereignty Rule Construction—With Discussion on China's Data Sovereignty Rule Con-

struction[J]. Modern Law Science, 2020, 42(06): 136-149.
[14] Liu Minmin. Reform of EU Personal Data Protection Directive and Its Enlightenment[D]. Southwest University of Political Science and Law, 2014.
[15] Chen Haibin, Wang Nuoya. Research on Japan's Cross-Border Data Flow Governance[J]. Information Studies: Theory & Application, 2021, 44(12): 197-204.
[16] METI Journal ONLINE. Resisting Data Hegemonism[EB/OL].[2023-03-16]https://journal.meti.go.jp/p/5894-2/.
[17] OFFICE of the USTR. Joint Statement of the Trilateral Meeting of the Trade Ministers of the European Union, Japan and the United States[EB/OL].[2023-03-05].https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/january/joint-statement-trilateral-meeting.
[18] Prime Minister's Office of Japan. Speech by Prime Minister Abe at the 25th International Conference on the Future of Asia Dinner[EB/OL].[2023-03-25]https://www.kantei.go.jp/cn/98_{abe}/statement/201905/*{00005}.html.*
[19] Zhang Xiaolei. Research on Japan's Cross-Border Data Flow Governance Issues[J]. Journal of Japanese Studies, 2020, 178(04): 85-108.
[20] Fang Kai, Mei Xiaying. Public Law Logic and Private Law Considerations for Government Data Opening[J]. Administration Reform, 2022, 154(06): 47-55.
[21] China Daily. U.S. Hegemony Harms Global "Digital Human Rights"[EB/OL].[2023-03-16]https://baijiahao.baidu.com/s?id=1742726950420381324&wfr=spider&for=pc.
[22] Jiang Xiaohong. Extraterritorial Application of EU Law: Value Objectives, Generation Paths, and Self-Limitation[J]. Chinese Review of International Law, 2022, 52(06).
[23] Li Haoen. On Extraterritorial Application of EU and U.S. Data Legislation and China's Response[J]. Peking University International and Comparative Law Review, 2021, 16(1): 157.
[24] Huanqiu. Opposing Data Hegemony and Enhancing Data Security Governance Capacity[EB/OL].[2023-03-19]https://baijiahao.baidu.com/s?id=1738379363420998520&wfr=spider&fo
[25] Zhang Li. Data Governance and Data Security[M]. Beijing: Posts & Telecom Press, 2020: 55-64.
[26] Cheng Hua, Wu Yufan, Li Sanxi. Data Trading and Data Monopoly: Based on Personalized Pricing Perspective[J/OL]. World Economy, 2023(03): 154-178[2023-04-04].https://doi.org/10.19985/j.cnki.cassjwe.2023.03.009.
[27] Scandal: Facebook Becomes Tool for Manipulating U.S. Election?[EB/OL].[2023-04-09]https://www.sohu.com/a/226229253{100119511}.
[28] Feng Zhaokui. China-U.S. Chip Competition: Reality, Logic, and Reflections[J/OL]. Asia-Pacific Security and Maritime Affairs: 1-20[2023-03-28]. https://doi.org/10.19780/j.cnki.ytaq.2023.2.2.
[29] Wang Lin. Decoding the National Data Bureau[N]. China Youth Daily, 2023-03-09(005).
[30] Mei Ao, Li Kunjia. Review of Japan's Data Security Governance System and Its Enlightenment[J/OL]. Information Studies: Theory & Practice: 1-8[2023-03-06]. http://kns.cnki.net/kcms/detail/11.1762.G3.20230203.1715.003.html.
[31] Wang Xue, Shi Wei. Globalization of Extraterritorial Jurisdiction in Data

Legislation and China's Response[J]. Intellectual Property, 2022, 254(04): 54-75.
[32] Kong Qingjiang, Yu Huayi. Phenomenon of Extraterritorial Application of Data Legislation and China's Response Strategies[J]. Law Science Magazine, 2020, 41(08): 76-88.
[33] Kong Qingjiang, Wang Chuqing. Global Governance of Cross-Border Data Flows: Lack and Construction of Inter-State Trust Relations[J]. Modern Communication (Journal of Communication University of China), 2022, 44(10): 65-70.
[34] Shen Wei, Feng Shuo. Globalism or Localism: Divergence, Game, and Coordination of Global Data Governance Rules[J]. Suzhou University Law Review, 2022, 9(03): 34-47.
[35] Li Hengyang. Analysis of Biden Administration's Cyberspace Strategy[J]. American Studies, 2022, 36(06): 98-116+7.
[36] Yu Yang, Liang Zheng. Global Data Flow, Protection, and China's Solutions[J]. Forum on Science and Technology in China, 2022, 319(11): 9-15.
[37] Liu Dian. Evolution, Development Trends, and China's Response to Global Digital Trade—From the Perspective of Cross-Border Data Flow Regulation[J]. Academic Forum, 2021, 44(01): 95-104.
[38] Huang Zhixiong. Legal Logic of Data Governance[M]. Wuhan: Wuhan University Press, 2021: 472-473.
[39] Wang Weiling. Government Data Authorized Operation: Practice Dynamics, Value Network, and Promotion Path[J]. E-Government, 2022, 238(10).

Author Contributions: LI Chengxi: Conducted policy research and drafted the paper; WU Xinnian: Proposed research ideas, designed the research framework, and revised the final version.

Note: Figure translations are in progress. See original paper for figures.