ANALYSIS OF THE CONFLICT BETWEEN DATA SOVEREIGNTY AND LONG-ARM JURISDICTION

Wang Cong
Doctoral Student at the University of World Economy and Diplomacy, Tashkent 100174,Uzbekistan
Suqian University, Suqian 223800, China
https://doi.org/10.5281/zenodo.16152543

Abstract: Data sovereignty and cross-border data flow governance have become key issues in the global digital age. This article analyzes the theoretical divisions and practical conflicts between data sovereignty and data freedom. On the one hand, the theory of data sovereignty extends from traditional sovereignty to technological sovereignty, emphasizing the state's jurisdiction over data; on the other hand, the theory of data freedom has been alienated in practice into the long-arm jurisdiction implemented by the United States and Europe through the Cloud Act and GDPR, forming a new type of digital hegemony. Research shows that the practices of various countries are divided into two models: the "indirect governance" of the European Union and the "direct control" of emerging countries, and there is a trend of mutual learning and integration. In the face of governance fragmentation caused by long-arm jurisdiction, countries need to build a data governance system that balances security and development, strengthen data cooperation through various innovative measures, and promote orderly flows while maintaining data sovereignty.

Keywords: Data sovereignty long-arm jurisdiction cross-border data flows global data governance GDPR

Introduction

In the digital age, data has become a national strategic resource and a core element of global competition. In the formulation of rules for cross-border data flows, the international community has gradually divided into two camps: "data sovereignty" and "data freedom", forming a complex pattern of theoretical opposition and practical conflict. Countries represented by China and Russia advocate data sovereignty and emphasize the jurisdiction and security control of data by the state; Europe and the United States extend domestic data rules to foreign countries through the "long-arm jurisdiction" mechanism, alienating "data freedom" into a new tool of digital hegemony. This opposition is not only reflected in the theoretical level, but also profoundly reshapes the global data governance practice. In this context, exploring a governance path that balances security and development has become a common issue for all countries.

Analysis and results

1. The conflict between data sovereignty and data freedom

The legal regulation of cross-border data flow has become a core issue in global digital governance, and its theoretical controversy has always revolved around a fundamental question: What kind of relationship should data and sovereignty maintain in the digital age? The answer to this question has differentiated into two completely different theoretical propositions - the "data sovereignty theory" that emphasizes state control and the "data freedom theory" that advocates free flow. These two theories not only represent the difference in the understanding of the nature of data, but also reflect the strategic orientation and value stance of different countries in the digital field.

1.1 Data sovereignty theory: the extension and evolution of traditional sovereignty in the digital age

The classic concept of sovereignty has become the cornerstone of the modern international order after the establishment of the Westphalian system. When Internet technology gave birth to the virtual "fifth space", a fundamental question arose: Can the sovereignty principle of the real world be applied to cyberspace without physical boundaries? Data sovereignty theorists gave a positive answer. [1] They believe that although data exists in the form of bits, its generation, storage and processing always rely on physical infrastructure, and these facilities must be located within a specific territory. Just as cyber sovereignty is the projection of traditional sovereignty in cyberspace, data sovereignty is the embodiment of sovereignty in the data field. [2]

Early discussions on data sovereignty were often intertwined with network sovereignty. In 2020, the EU successively released three documents, including the European Data Strategy, proposing the concept of "technological sovereignty", pushing the theory of data sovereignty to a new level. [3] The proposal of technological sovereignty reflects the maturity of the theory of data sovereignty, which has evolved from the initial assertion of jurisdiction to a systematic theoretical framework covering technology, rules, and values. This evolution shows that data sovereignty is not a static concept, but a dynamic system that is constantly enriched with the development of technology. [4]

1.2 Data Freedom Theory: The Paradox of Ideal and Reality

In sharp contrast to data sovereignty theory is the "data freedom theory" that originated from the utopian thought of the early Internet. The prototype of data freedom theory can be traced back to the "Declaration of the Independence of Cyberspace" published by John Barlow in 1996, which declared that

"cyberspace is not within your borders." Early network theorists Johnson and Post proposed that the decentralized nature of cyberspace enables it to spontaneously form a legal order independent of real sovereignty. This view is based on technological determinism, believing that code is law and that the governance of cyberspace should be dominated by the technical community rather than the government. At the economic level, data freedom theory is supported by neoliberal theory. [5]

The fundamental contradiction facing the theory of data freedom is that the "de-sovereignization" it advocates needs to be achieved through legislation by sovereign states. When the United States passed the "Cloud Act" to extend its data jurisdiction beyond its borders, it was actually promoting anti-sovereignty ideas by sovereign means. This "self-denial" has led to the alienation of the theory of data freedom into a tool of digital hegemony in practice.

The confrontation between data freedom and sovereignty is essentially a conflict of different values. The United States regards data mainly as an economic asset, the European Union emphasizes its relationship with human rights, and China attaches importance to the relationship between data and national security. These differences are due to their respective historical traditions and actual national conditions.

The debate on data sovereignty and freedom is not just a theory, but directly shapes the global data governance landscape. To understand this theoretical division, we need to grasp three key points: [6]

First, both theories have their rationality and limitations. Completely denying sovereignty may lead to digital anarchy, while absolutely emphasizing sovereignty may stifle innovation vitality. The ideal model should be to find a dynamic balance between the two.

Second, the choice of theoretical position is closely related to the stage of national development. Digital powers tend to allow free flow to expand their influence, while latecomers need more sovereign barriers to cultivate local industries. This difference makes data governance a new battlefield for international competition.

Finally, theories are interpenetrating in practice. The European Union has both maintained data sovereignty and established global influence through GDPR; while China insists on data sovereignty, it is also piloting measures to facilitate cross-border data flows in free trade pilot zones. This convergence foreshadows a complex landscape for future data governance.

2. Practical expression: two paths to achieve data sovereignty

In the process of transforming theory into practice, data sovereignty presents two typical paths to achieve it: one is the "indirect protection of rights" model represented by the European Union, which emphasizes guiding market self-discipline through high-standard legislation; the other is the "sovereign direct participation" model represented by China, Russia and other countries, which directly intervenes in data governance through mandatory regulations. These two paths reflect the differences in different legal traditions and governance concepts, but both successfully bring virtual data into the jurisdiction of national sovereignty.

2.1 EU model: indirect governance based on rights protection

The EU's data governance system is built on a profound tradition of rights protection. Its General Data Protection Regulation (GDPR) has pioneered an innovative path of "realizing sovereignty through private rights". This mechanism includes three key designs: high-standard legislation to establish behavioral norms, diversified compliance mechanisms, and a hierarchical regulatory system. The subtlety of this model lies in the fact that state power is hidden behind the rights protection framework, and market players are guided to independently realize their sovereign will by setting the rules of the game. [7] The case of the EU's fine of 746 million euros on Amazon in 2021 shows that this "light-touch regulation" can also produce a strong deterrent effect.

2.2 Mandatory localization model: direct manifestation of sovereign power

Unlike the EU's indirect governance, many countries choose to directly exercise sovereign power through data localization storage requirements. This model presents diverse characteristics in legislative techniques and implementation mechanisms. From the perspective of legislative genealogy, there are strict types in all fields, such as Russia; there are types that focus on key areas, such as China; and there are types that regulate specific industries, such as Australia. From the perspective of the law enforcement toolbox, countries have developed distinctive law enforcement methods to implement localization requirements. For example, China adopts technical review, establishes a cybersecurity review system, and conducts data security assessments on companies listed overseas; India uses economic leverage to require payment data to be processed domestically, otherwise the payment license will be revoked; France adopts judicial deterrence. [8]

2.3 Comparison of models and convergent development

The two paths have their own advantages in terms of implementation effect: the EU model is more adaptable to global business needs, and although the compliance costs of enterprises are high, market expectations are clear; the localization model can quickly respond to national security concerns, but may increase corporate operating costs. Interestingly, in recent years, there has been a trend of mutual learning and integration: the EU strengthens the sovereignty element, and Article 48 of the GDPR explicitly refuses to enforce foreign court rulings that conflict with EU law, which is essentially a declaration of sovereignty. The Data Governance Act requires that specific public interest data must be processed within the EU. The hybrid model is also gradually emerging. Saudi Arabia adopts the "data classification + geographic mirroring" strategy: original data must be stored domestically, but overseas backup is allowed; data in sensitive industries such as finance is strictly localized.

This convergence phenomenon shows that in global data governance practices, neither pure free flow nor absolute sovereign control can stand alone, and countries are exploring a "third way" to balance security and development.

3. Practical alienation: the paradox of data freedom and long-arm jurisdiction

The theory of data freedom has shown obvious alienation in practice: the theory that originally advocated "de-sovereignty" has eventually evolved into a tool for some countries to expand their extraterritorial jurisdiction. The most typical manifestation of this alienation is the data long-arm jurisdiction mechanism established by the United States and the European Union through domestic legislation, which is essentially "sovereignty expansion" in the name of "data freedom".

3.1 Legal mechanism of long-arm jurisdiction

Jurisdiction in traditional international law is mainly based on the territorial principle and the personal principle. However, in the field of data, the United States has reconstructed the basis for jurisdiction through the "data controller standard". [9] The new rule established by the 2018 "Clarifying Lawful Extraterritorial Use of Data Act" (CLOUD Act) is that as long as the data controller (such as a technology company) is subject to the jurisdiction of the United States, the US government has the right to retrieve the data regardless of where it is actually stored. This is equivalent to shifting jurisdiction from geographical space to legal relationship space.

3.2 Conflict of rules and sovereignty confrontation

In order to deal with long-arm jurisdiction, many countries have enacted blocking laws. China's Anti-Foreign Sanctions Law explicitly prohibits the implementation of discriminatory restrictive measures against foreign countries. The revised version of the EU Blocking Regulation includes the US Cloud Act in the appendix. Russia stipulates that foreign data requests must be reviewed by Russian judicial authorities. Long-arm jurisdiction has given rise to counter-technical measures. China promotes the de-"IOE" (IBM, Oracle, EMC) of IT facilities in the financial, telecommunications and other industries. The EU GAIA-X project builds an independent cloud infrastructure. Russia's Runet Act establishes a national domain name resolution backup system.

The institutional root of this alienation phenomenon is the deviation of value goals. The original pursuit of data freedom theory is to break down sovereignty barriers, but in practice it has been alienated into the United States to maintain the global competitive advantage of technology companies and the EU to expand the scope of influence of regulatory standards. Both have deviated from the original intention of the theory and become digital geopolitical tools.

This alienation phenomenon foreshadows the fundamental dilemma facing global data governance: when the theory of data freedom is alienated into a tool for expanding jurisdiction, it actually exacerbates rather than eliminates the division of digital space. The 2021 United Nations Conference on Trade and Development report pointed out that the world has formed three data governance circles centered on China, the United States and Europe, each of which implements different jurisdictional rules. This state of "digital fragmentation" is far from the vision of interconnection pursued by the founders of the Internet.

Conclusion

The theoretical division and practical conflict between data sovereignty and long-arm jurisdiction profoundly reflect the tension between national sovereignty and globalization in the digital age. Starting from the traditional sovereignty principle, the theory of data sovereignty continues to expand its theoretical boundaries through new forms such as technological sovereignty; while the concept of data freedom has been alienated in practice into a tool for some countries to expand their extraterritorial jurisdiction. This opposition has not only caused the fragmentation of global data governance, but also triggered multiple games among countries at the legislative, judicial and technical levels.

The international order in the digital age is being reconstructed, and the

dispute over data sovereignty will become an important dimension of this process. Only by respecting the differences in the development stages of various countries and adhering to the cooperative spirit of multilateral consultation can we achieve the co-governance and sharing of digital space and ultimately build a community of shared future in cyberspace.

References

1. Perritt, Henry H. Jr. The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance[J], 5 Indiana Journal of Global Legal Studies 423, 425, 1998.

2. Zhi Zhenfeng. Internet sovereignty is rooted in modern legal theory[N], Guangming Daily, December 17, 2015, p. 004.

3. Shaping Europe's digital future, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273, May 7, 2025.

4. Qi Aimin, Pan Jia. The establishment of data rights, data sovereignty and the basic principles of big data protection [J], Journal of Suzhou University (Philosophy and Social Sciences Edition), 2015 (01) : 64-70.

5. Jiang Tao. Datafication: Intelligence from the inside out [M], Communication University of China Press Co., Ltd. 2018 edition, pp. 14-26

6. Manyi Qi. The international pattern of cross-border flow of personal data regulation and China's response [J], "Legal Forum" 2018（03） : 130-137;

7. General Data Protection Regulation, Article 1 and Articles 44-50, https://gdpr-info.eu/, 2020-03-07.

8. Hong Yanqing. Constructing a security assessment framework for cross-border data flow in the balance between development and security [J], Information Security and Communication Confidentiality, 2017 (02) : 32-62.

9. Guo Yujun, Xiang Zaisheng. The long-arm jurisdiction of US courts in cyber cases [J], China Legal Science, 2002 (06) : 155-168.