Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/16/20231127

Long-Arm Jurisdiction in Cross-Border Data Flows: EU-US Gaming and Balancing

Yuxin Tian[1,a,*,†], Hanwen Zhang[2,b,†]

[1]*Department of French, University of International Relations, Beijing, 100091, China*
[2]*Department of Chinese Language and Literature, Tianjin University, Tianjin, 300354, China*
a. yuxintian@uir.edu.cn, b. 3021002049@tju.edu.cn
**corresponding author*
[†]*These authors contributed equally.*

Abstract: In the era of digital economy, the power struggle and legal challenges arising from cross-border data flows have become increasingly prominent, making data governance a focal topic in the international community. Countries are competing and cooperating in formulating rules on cross-border data flows, as this phenomenon becomes more significant with the global popularity and rapid development of big data-based digital products like ChatGPT. As traditional powers in this field, the United States and the European Union have established long-arm jurisdiction systems with unique characteristics and have engaged in multiple rounds of fierce gamesmanship over dominance in global data flow governance standards, while constantly seeking power balance in bilateral cooperation. Through historical research, comparative analysis, and case studies, this paper analyzes and summarizes the governance principles, regulatory models, and competitive and compromising processes of transatlantic data flows, leading to the conclusion that China's data governance strategy should balance data security and data freedom, while transforming its approach to regulating data outflows and emphasizing the importance of efficiency values in maintaining data sovereignty. By expanding international cooperation and promoting the signing of regional data flow agreements, China can enhance its voice in the global data governance system.

Keywords: cross-border data flows, long-arm jurisdiction, cyber sovereignty, GDPR, CLOUD Act

1. Introduction

In March 2023, Italy imposed a temporary ban on OpenAI's ChatGPT product, citing violations of the *General Data Protection Regulation* (GDPR). This case highlights the intricate and daunting challenges of cross-border jurisdiction in the digital age, prompting a re-examination of the legal frameworks and principles surrounding extraterritoriality and long-arm jurisdiction in the context of international data flow regulations. Currently, the correct solution for China to address the pressure of extraterritorial jurisdiction enforcement still requires further discussion. Hence, it is imperative to analyze and assess the development trends of the international extraterritorial jurisdiction mechanism, promoting a more comprehensive and sound flow and protection of data in China.

This paper begins by outlining the emergence and historical development of long-arm jurisdiction (Section 2), with particular attention to its impact on the sovereignty of cyberspace states. Using

DOI: 10.54254/2753-7048/16/20231127

GDPR in the European Union (EU) and the *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) in the U.S. (U.S.) as primary examples, the evolution of long-arm jurisdiction in cross-border data flow regulations is analyzed (Section 3). By examining the differences in the long-arm jurisdiction practices between the EU and the U.S., this paper identifies divergent underlying logics of data governance (Section 3.3). The discussion then shifts to the competition and cooperation between the EU and the U.S. in data flow regulation (Section 4). Firstly, the EU's construction of "digital sovereignty" in response to the U.S.'s offensive strategy is discussed (Section 4.1). Secondly, the strategy of the U.S. is explored around the negotiations of the *Trans-Atlantic Data Privacy Framework* (TADPF) and the signing of the Cross-Border Privacy Rules System (CBPRs) (Section 4.2). Finally, this paper proposes strategies for China to cope with extraterritorial long-arm law enforcement pressure (Section 5), including enhancing domestic legislation, transforming governance paradigms, and strengthening international cooperation.

The exploration of the broader legal implications of long-arm jurisdiction and the analysis of the competition and cooperation between the U.S. and the EU aim to provide insightful and informative perspectives on the challenges and opportunities presented by the constantly evolving patterns of trans-border data flow and digital sovereignty.

2. The Emergence and Development of Long-Arm Jurisdiction

2.1. The Origin and Evolution of Long-Arm Jurisdiction

"Long-arm jurisdiction" originated in American civil procedural law, derived from traditional personal jurisdiction, and has gradually been established through case law and legislation since the mid-20th century. In International Shoe Co. v. State of Washington, the "minimum contacts" standard for asserting civil jurisdiction was established by the U.S. Supreme Court [1]. This means that as long as there are minimum contacts between the defendant and the jurisdiction where the court is located, ensuring that the litigation does not violate traditional notions of fairness and justice, the court can exercise personal jurisdiction over non-resident defendants and serve legal documents. The civil jurisdiction rules established based on this principle are figuratively called "Long Arm Statutes."

As editor-in-chief of Black's Law Dictionary, Bryan A. Garner defines it as the jurisdiction enjoyed by a court over a defendant who does not reside in the court's jurisdiction but has some connection with it [2]. This concise explanation, however, is only from a judicial perspective and does not cover the complete contemporary meaning of the concept of long-arm jurisdiction. Within the scope of digital law, long-arm jurisdiction has evolved beyond its initial concept in American civil procedural law, becoming synonymous with "extraterritorial jurisdiction," which includes extraterritorial legislation, enforcement, and adjudication. Its exercise in cyberspace and its infringement upon national sovereignty have long been of concern to various countries.

2.2. Long-Arm Jurisdiction in Cyberspace

Due to the virtual, open, and global nature of the internet, its advent and popularization have broken the traditional geographic boundaries of national sovereignty. The international community has been exploring and negotiating the establishment of "cyberspace sovereignty" for many years, and its status as a component of national sovereignty has been widely recognized by various countries [3]. As a subset of cyberspace sovereignty, although "data sovereignty" is controversial, it is a common practice for sovereign states to maintain and exercise it [4].

Sovereign states use long-arm jurisdiction to regulate cross-border data flows, extending jurisdiction to extraterritorial actions or entities. On the one hand, this is beneficial for maintaining national sovereignty and data security, as well as protecting the public interest and citizens' rights; on the other hand, it may infringe on other countries' cyberspace sovereignty and data sovereignty,

DOI: 10.54254/2753-7048/16/20231127

inevitably leading to numerous legal conflicts and international disputes. Based on this, the competition between various countries' cross-border data flow regulations is intense, with the long-arm jurisdiction featured in both the EU and the U.S. legal practices being the most representative.

3. Different National Approaches Implementing Long-Arm Jurisdiction

In the field of regulatory frameworks governing the movement of data across international borders, the EU and the U.S. each attempt to shape international rules based on their respective domestic legal systems and national values. The EU focuses on protecting the rights of data subjects, namely privacy rights, while the U.S. places greater emphasis on expanding government power [5]. Although their paths may seem significantly divergent, they are essentially competing for the same goal: the authority to establish universal rules for cross-border data flows.

3.1. The EU GDPR

3.1.1. A Defensive Protection of Private Rights

The EU's GDPR, enacted in 2016 and in effect since 2018, is widely regarded as "the strictest data protection regulation in history." It significantly expands the jurisdiction of European data protection regulators. The GDPR adopts the principle of extraterritorial jurisdiction, extending its long arm of jurisdiction over data controllers and processors outside the EU based on the effectiveness principle, with a protective jurisdictional hue. This encompasses all entities that offer products or services to individuals within the EU or engage in monitoring the behaviors of EU individuals. This means that any organization processing the personal data of citizens, regardless of whether it is located in the EU, may be subject to the regulation. The purpose of the law is to protect EU citizens from unlawful violations of their personal information by introducing defensive legislation to protect their right to privacy.

3.1.2. The Goal of Global Governance

Long-arm jurisdiction is one of the key factors for the GDPR to achieve the "Brussels Effect." Given the vast user base of the digital economy within the EU and beyond, the GDPR's effectiveness has global applicability and enforceability. Furthermore, nearly 70 countries outside the EU have adopted or transplanted this model [6]. As a result, the EU has become the leader in setting global data regulation rules, and to some extent, the EU model has achieved the goal of global governance [7].

3.2. The U.S. CLOUD Act

3.2.1. An Offensive Exploration of Public Power

Unlike the GDPR, the long-arm jurisdiction embodied in the CLOUD Act reflects the offensive exploration of U.S. public power in the jurisdiction. In 2018, the U.S. enacted the CLOUD Act as an amendment to the *1986 Electronic Communications Privacy Act* (ECPA). The act abandons the international standard of solely focusing on the "location of data storage" and instead advocates the "data controller" standard, explicitly authorizing U.S. law enforcement agencies to require data service providers to preserve, back up, or disclose data they own, oversee, or control, regardless of whether such data is stored within or outside the U.S. . This means that the U.S. government has been granted unilateral access to extraterritorial data and can extend its jurisdiction over global data through the extensive data storage networks of U.S. companies.

DOI: 10.54254/2753-7048/16/20231127

3.2.2. The Pursuit of "Efficiency"

The white paper released by the U.S. Department of Justice in April 2019 states that the primary aim of the COULD Act is to enhance the "efficiency" of a certain process or system of cross-border data collection to combat the growing problem of cybercrime [8]. However, efficiency alone is not a sufficient legal basis for violating the privacy of foreign citizens, the data rights of enterprises, and the sovereignty of other countries in cyberspace. This unilateral and controversial approach to legalizing cross-border data collection has been widely criticized and questioned in practice [9].

3.3. The Causes of Different Practices of Long-Arm Jurisdiction

Both European and American regulations on data cross-border flow contain long-arm jurisdiction elements, but their cores are markedly different, reflecting the underlying divergences in their governance logic for cross-border data flow regulation.

3.3.1. The EU Defends Its Global Influence Through Human Rights Protection

The EU has taken a more "data protectionist" approach. On the one hand, in European traditional legislative and judicial practices, personal data protection is inseparable from human rights protection, which is based on the unique European concept of human dignity [10]. Both the *Charter of the EU* and the *Charter of Fundamental Rights of the EU* explicitly stipulate the right to privacy and personal data protection, providing a constitutional-level legal basis for GDPR's adoption of long-arm jurisdiction to safeguard the human rights of EU citizens. Conversely, the digital economy of the EU is located at the periphery, as evidenced by its representation of merely 4% of the market value of the world's 70 largest digital platforms (the U.S. and China account for 90%), making it the most significant exporter of information globally, posing a threat to the EU's economic development and security [11]. Consequently, the GDPR, based on the high standard of human rights protection, expands the global influence of the EU model through the implementation of long-arm jurisdiction and adequacy determination to reverse its disadvantageous position in the global Internet industry. In 2022, the EU positioned itself as the "global standard-setter" in cross-border data flows, aiming to shape international data flow standards that align with EU values and interests, establishing a discourse system to counter the U.S. offensive while resisting it [12]. Europe deliberately makes Human Rights one of the core values of its global strategy, to the extent that American scholars have pointed out that this advocacy is not due to moral superiority, but rather because it is the only means at hand to solve problems [13].

3.3.2. The U.S. Quests for Global Data Dominance via Data Free Flow

The U.S. is the foremost advocate of "data liberalism," pioneering the concept of a "borderless" and "extraterritorial" global common in cyberspace and promoting a "multi-stakeholder governance model" [14]. For a long time, the U.S. has attempted to promote the free cross-border flow of global data and implement long-arm jurisdiction for reasons such as "improving efficiency" and "promoting trade." Relying on U.S. high-tech companies that provide services globally and control massive data, the U.S. government can use "data free flow" as a shield to employ the long-arm jurisdiction principle and request data controllers for extraterritorial data, effectively monitoring and managing global data. The ultimate goal of this model is to seize the discourse and control of global data flow rules and dominate cyberspace through advanced network technology and a developed digital economy.

The different practices of long-arm jurisdiction in the data flow regulations of the U.S. and the EU are not only due to the different choices made between efficiency and human rights, but also due to

DOI: 10.54254/2753-7048/16/20231127

their common goals of safeguarding national security, consolidating their positions in the world digital economy, and the fierce competition for leadership in global data flow regulation.

4. EU-U.S. Competition and Cooperation

As two dominant players in global data flows, the EU and the U.S. vie for supremacy in global cyberspace through legal and technological means while actively establishing bilateral cooperation mechanisms to maximize their respective national interests in cross-border data flows.

4.1. EU Strategy: Establishing "Digital Sovereignty"

Confronted with the U.S.'s aggressive long-arm jurisdiction tactics aimed at seizing control over global data, the EU responds by introducing the concept of "digital sovereignty" into its political discourse [15]. The EU implements a series of measures at the regulatory and technological levels to assert the authority, autonomy, and effectiveness of European data governance and to consolidate Europe's position in international competition in the digital age.

4.1.1. Regulatory: Development of the Principle of Protection

In negotiations with the U.S. to establish a bilateral mutual recognition mechanism, the EU applies the principle of adequacy stipulated in EU law to exert pressure on the U.S. Notwithstanding the fact that the Safe Harbor and the Privacy Shield were signed, both were later invalidated by the Court of Justice of the European Union (CJEU) due to the U.S.'s inability to ensure full data protection. This, in fact, highlights the EU's advantageous position in the game of cross-border data flow regulation between the EU and the U.S. and is a strong repudiation of European data protectionism, which is focused on privacy protection, and US-style data liberalism. Additionally, after the EU Network and Information Security Act was passed in 2019, the EU Network and Information Security Agency (ENISA) is developing the EU Cybersecurity Certification Scheme on Cloud Services (EUCS), a pan-European certification framework that mandates cloud service providers to localize their business and infrastructure within the EU to indirectly achieve data localization [16]. This is a strong measure taken by Europe to avoid US long-arm jurisdiction.

4.1.2. Technological: Blueprint for Digital Infrastructure Autonomy

The EU also strives to achieve "technological sovereignty" over network infrastructure by developing digital technology to reduce dependence on US companies and to ensure that EU data is not subject to third-country laws due to being stored on foreign data platforms. The Gaia-X Project, jointly released by the German and French economy ministers in 2020, is a flagship project aimed at promoting the development of digital infrastructure in Europe and creating a self-sustaining ecosystem for European data and artificial intelligence [17]. However, the plan has encountered many obstacles in practice: firstly, there are differences of opinion among EU member states; secondly, due to the long-term dominance of US digital giants in the EU market, which hold nearly 70% of the market share, and the participation of several Chinese technology companies, Gaia-X has deviated from its original goal of effectively cultivating and supporting European cloud service providers. In fact, the plan has shifted from cultivating a "European-owned" digital ecosystem to establishing a global digital ecosystem "operated in Europe [18]."

4.2. U.S. Approach: Promoting the Value of Data Free Flow

The U.S., the leading promoter of cross-border data flow, has been striving to alleviate the concerns and opposition of international entities, such as the EU, regarding data liberalism. On the one hand,

DOI: 10.54254/2753-7048/16/20231127

the U.S. has made concessions to the EU to facilitate consensus between the two parties, and on the other hand, it has actively promoted the signing of multilateral agreements on cross-border data flow to achieve the goal of eliminating barriers in cyberspace and seizing the dominant position in the global cyberspace.

4.2.1. US-EU Bilateral Agreement: New Commitments

Following the failures of the Safe Harbor Agreement and the Privacy Shield Agreement, the EU and the U.S. reached the Trans-Atlantic Data Privacy Framework (TADPF) in March 2022 after multiple rounds of negotiations. This is the latest development in the U.S.-EU game in the field of cross-border data flow regulation, and the two parties have reached a principled consensus on the agreement. The U.S. has promised to implement new protection measures, including strengthening the protection of citizens' privacy and freedom in its signal intelligence activities, establishing independent and binding new remedies for EU citizens, and strengthening hierarchical supervision of signal intelligence activities [19]. In October 2022, US President Biden signed an executive order to implement these commitments in writing, as the basis for the EU Commission's assessment of the adequacy of protection, but whether the framework can pass the test of the EU Court of Justice remains uncertain.

4.2.2. Regional Multilateral Cooperation: Enhancing Dominance

The U.S. has promoted its own values of digital liberalism through trade negotiations and has emphasized this important principle in multiple regional cooperation agreements. In addition to the U.S.MCA, in 2004, the U.S. led and facilitated the signing of the first regional guiding document on cross-border data flow regulation in the Asia-Pacific region - the APEC Privacy Framework, which aims to promote e-commerce development in the Asia-Pacific region and achieve cross-border data flow within the region. In 2012, the U.S. vigorously promoted the APEC Cross-Border Privacy Rules System (CBPRs), forming a more mature multilateral regulatory mechanism, and thus moving closer to the goal of data liberalization.

Undoubtedly, the EU has leveraged its dominant regulatory power within the large single digital market to promote its digital governance norms and values, which has achieved certain results in restraining the U.S. However, the complex and diverse regulatory mechanisms cannot directly drive the development of the EU's own digital technology. Without strong technological support, the EU is almost impossible to solely rely on rulemaking to gain decision-making power in global data governance issues [18]. On the other hand, the U.S., relying on its developed digital industry foundation, seeks to quickly reach mutual recognition with the EU through partial concessions, and actively promotes its national values in international agreements in the hope of establishing its dominance in cyberspace.

5. China's Regulatory Plan for Data Flow

With the increasing participation of emerging countries in cyberspace governance, the traditional legislative paradigm dominated by Europe and the U.S. is continuously being disrupted and reshaped, and a new global legal system for data governance is emerging [20]. In this context, to better address the long-arm jurisdictional pressure from outside its jurisdiction, China should establish a regulatory framework that balances data freedom and data security and provide its own expertise for establishing a regional or even global universal data flow governance scheme.

DOI: 10.54254/2753-7048/16/20231127

5.1. Various Approaches to Constructing "Data Sovereignty"

China can draw inspiration from the EU's promotion of digital sovereignty and technological sovereignty in shaping the order of "data sovereignty". Firstly, at the technical level, it can actively promote legislation to support the construction and development of digital economy technology and infrastructure and reduce its dependence on foreign companies. Secondly, at the rule level, it can continuously improve its domestic legal framework for data outflow and establish blocking laws for long-arm jurisdiction. The legislative body can also establish a whitelist system for reviewing the eligibility of data recipient countries based on the "adequacy protection" assessment of GDPR, which would appropriately reduce approval procedures for countries or regions that meet the standards and impose strict restrictions or even control on countries and regions with high risks of data flow. Thirdly, in practice, it is most important to supervise domestic companies to improve their compliance with the *Measures for Security Assessment for Outbound Data Transfer* issued in 2022.

5.2. The Evolution of Data Export Control Thinking

The legal model for the development of cyberspace in a sustainable manner cannot be based on the monopolistic spatiality of territorial sovereignty. The crucial role of the "efficiency" value of the digital economy era cannot be overlooked. Overly rigid adherence to traditional sovereignty and mandatory data localization will destroy the basic characteristics of the Internet's interconnection and intercommunication, leading to Cyber-balkanization (also termed internet Balkanization) [21]. Compared to the U.S. and Europe, which actively seek international discourse power through long-arm jurisdiction, China is still in a passive situation and closely tied to its long-standing regulatory thinking of emphasizing security and neglecting freedom [22]. Therefore, when legislating, China should increase the free flow of data under adequate jurisdiction, find a balance between protection principles and efficiency needs, avoid creating unnecessary trade barriers in the digital market, and reduce data transaction costs. It should also shift from a passive defense mode that emphasizes data localization to an active mode that equally emphasizes security and freedom to gain a strategic advantage in global competition.

5.3. Active Participation in International Data Governance Cooperation

Since data flow issues have a natural global nature, balancing data freedom and data security through bilateral or multilateral agreements and gradually incorporating data flow rules into international legislative frameworks is an inevitable trend. China can learn from the relevant practices of the U.S. and actively promote the signing of regional and international data flow agreements. For example, relying on bilateral or multilateral cooperation mechanisms such as the "Belt and Road Initiative," China can select countries and regions with good political and economic mutual trust and sound data rule of law to conduct data flow negotiations and reach consensus, driving the formation of regional and even global agreements and building a community of shared destiny in the global cyberspace.

6. Conclusion

Cross-border data flows are becoming an important feature of the new globalization, a focal issue in the latest iteration of global economic and trade regulations, and a strategic frontier of great power competition. Influenced by factors such as geopolitical concerns, national security, privacy considerations, and industrial development levels, the U.S. and the EU, while both adopting long-arm jurisdiction, serve different objectives of data protectionism and data liberalism, respectively. Analyzing the game and balance surrounding cross-border data flow regulation in the U.S. and Europe can provide valuable reference and inspiration for China to improve its regulatory system for

DOI: 10.54254/2753-7048/16/20231127

cross-border data flows, helping achieve its goal of increasing its international discourse power in the digital economy and building a "digital economic power." However, with the ongoing fierce negotiations between the U.S. and Europe, it is difficult to determine whether the TADPF can be signed smoothly, making the prospects of cooperation uncertain. Furthermore, the EU is still implementing and improving technical and regulatory data protection measures in response to those established by the U.S., so the ultimate effectiveness of these policies and regulations requires time to verify. The proposed Chinese data governance plan in this paper also requires ongoing observation and evaluation based on changes in domestic and international situations for its operational and effective implementation.

References

[1] *International Shoe Co. v. State of Washington, 326 U.S. 310 (1945). Washington, D.C.: U.S. Supreme Court.*

[2] *Garner, B. A., & Henry Campbell Black. (2021). Black's law dictionary. Thomson Reuters.*

[3] *Schmitt, M. N. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.*

[4] *Zhu, Y. (2021). Reinterpretation of data sovereignty in the context of Data Security Law. Journal of Zhejiang University of Technology (Social Sciences), 20(4), 418–424.*

[5] *Wu, X. (2021). The Construction of Cross-Border Rules for Personal Information Based on the Perspective of Data Sovereignty. Tsinghua University Law Journal, 15(3), 74–91.*

[6] *Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Ministry of Electronics and Information Technology, Government of India.*

[7] *Safari, B. A. (2016). Intangible privacy rights: How Europe's GDPR will set a new global standard for personal data protection. Seton Hall Law Review, 47(3), 812.*

[8] *United States Department of Justice. (2019). Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. Retrieved from https://www.justice.gov/criminal-oia/page/file/1153436/download.*

[9] *Liu, T. (2020). Theoretical Distinctions and Practical Conflicts Between Data Sovereignty and Long-arm Jurisdiction. Global Law Review, 2020(02), 180–192.*

[10] *Basic, M. (2019). The Age of Dignity: Human Rights and Constitutionalism in Europe. Zbornik Radova Pravnog Fakulteta Splitu, 56(1), 269-II.*

[11] *United Nations Conference on Trade and Development. (2019). Digital Economy Report 2019 - Value Creation and Capture: Implications for Developing Countries. United Nations Publications.*

[12] *European Commission. (2022). An EU Strategy on Standardization: Setting Global Standards in Support of a Resilient, Green and Digital EU Single Market. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661.*

[13] *Kagan, R. (2004). Of Paradise and Power: America and Europe in the New World Order, Vintage.*

[14] *Clinton, H. R. (2010). Remarks on Internet freedom. Retrieved from https://2009-2017.state.gov/secretary/2009-2013clinton/rm/2010/01/135519.htm.*

[15] *Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(2), 230-246.*

[16] *European Union. (2020). European Cybersecurity Certification Scheme for Cloud Services. Retrieved from https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.*

[17] *European Commission. (2020). Declaration: Building the Next Generation Cloud for Businesses and the Public Sector in the EU. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70089.*

[18] *Gong, Y. (2022). The Return of the Sovereignty Concept in Digital Era and the EU's Digital Governance. Chinese Journal of European Studies, 2022(3), 18-48+165+6.*

[19] *The White House. (2022). United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/.*

[20] *De Burca, G., Keohane, R. O., & Sabel, C. (2013). New modes of pluralist global governance. New York University Journal of International Law and Politics, 45(3), 723-786.*

[21] *Hill, J. F., & Noyes, M. (2018). Rethinking Data, Geography and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls. New America.*

DOI: 10.54254/2753-7048/16/20231127

[22] Chen, T. (2023). The Challenges of and Solutions to Cross-Border Data Outflows Under the Pressure of Long-Arm Practice. Journal of Shanxi Normal University (Social Science Edition), 50(2), 101–112.