Vol.3 No.1 2022
https://doi.org/10.37420/j.cer.2022.002
Communication & Education Review

Data Risk and its Response Under the Long-arm Criminal Jurisdiction Threshold

Linyi Xu*
School of Law, Beijing Normal University, Beijing, China
*Corresponding author, email: 1304739872@qq.com

Abstract: *The expansion of long-arm criminal jurisdiction in the data field has brought data risks to other countries. In the context of cross-border data transfer, China is also faced with new risks such as the inherent lack of data protection of criminal law and the weakening of data regulatory ability. In this regard, China should create legal benefits in legislation, appropriately expand the effect outside the criminal law, refine its provisions on data sovereignty, improve the criminal policy of protecting data sovereignty, and draw on international experience to timely resolve data risks under the long-arm criminal jurisdiction of the United States.*

Keywords: *Information Age; Long-arm jurisdiction; Criminal jurisdiction;Data risk*

Introduction

With advanced science and technology, a perfect legal system, strong economic capital, and expanding international discourse power, the United States has established a significant long-arm criminal jurisdiction system by continuously extending its jurisdiction in judicial practice. With the advent of the era of big data, the long-arm criminal jurisdiction shows a trend of further expansion, and its scope of application has expanded to the data field, forming data hegemony and bringing risks to data security in other countries. The Meng Wanzhou incident, which has attracted widespread national attention, US sanctions against ZTE and Microsoft's acquisition of TikTok in the United States, mean that the United States is using this jurisdiction to interfere in China's data technology development and data supervision, and China is in a passive negative position in data protection. Data security has become more concerned about new resources and new opportunities, our country also attaches more attention to data security, 2021, the People's Republic of China for national economic and social development of the fourteenth five-year plan and 2035 vision target outline, "improve the national network security laws, regulations, and standards, strengthen data resources in important areas, important network and information system security" and promote "digital and cyberspace international rules". This paper studies the characteristics and development trend of American long-arm criminal jurisdiction in the information age explores the risks caused to China and assumes the countermeasures for China according to the risks.

The Deconstruction and Unity of the Concept and Characteristics of Long-arm Criminal Jurisdiction

In the face of data virtuality, the traditional concept of jurisdiction is easy to be blurred and interpreted in the context of big data, and there is a dilemma of application. And the existing research on long-arm jurisdiction

Vol.3 No.1 2022
https://doi.org/10.37420/j.cer.2022.002

is concentrated in the civil field, and the long arm jurisdiction research of the big data era is still not perfect, for the definition and use of long arm criminal jurisdiction concept is also different, so it is necessary to deconstruct long arm criminal jurisdiction concept and illustrate the characteristics of long arm criminal jurisdiction in the data era.

The Concept of Long-arm Criminal Jurisdiction

Long-arm criminal Jurisdiction refers to long-arm jurisdiction applicable in criminal cases. Long-Arm Jurisdiction (Long-Arm Jurisdiction), an expanded jurisdiction where the jurisdiction of the court cannot hear the case by a rule of territorial jurisdiction, but the court of the court has some minimum connection with the court through long-arm jurisdiction. In the subsequent development, the adjustment scope of long-arm jurisdiction is not limited to cases between domestic states but has jurisdiction over foreign cases to form the unique long-arm jurisdiction system of the United States. With the continuous application of long-arm jurisdiction in practice, the application of this system is not limited to civil cases but gradually expanded to criminal cases to form long-arm criminal jurisdiction. In the information age, the application of long-arm criminal jurisdiction has also expanded to the data field, taking jurisdiction over data rights and playing a role in related cases in the data field.

Long-arm jurisdiction is not the same as extraterritorial jurisdiction. They are completely different concepts, with differences in the subject of exercise, type of jurisdiction, and legal basis. Long-arm jurisdiction and long-domain jurisdiction differ greatly from the scope of application in the data field. The former is far higher than the latter. In the information age, the development trend of long-arm jurisdiction is also different from off-domain jurisdiction, and these differences determine that China cannot treat rapidly changing long-arm jurisdiction only in the way of off-domain jurisdiction.

Table1. The distinction between out-of-domain jurisdiction and long-arm jurisdiction

Jurisdiction name	Long arm jurisdiction	Extraterritorial jurisdiction
The subject of exercise is different	It is often exercised by the courts	The Legislature, judicial organs, and administrative organs exercise separately
The types of jurisdiction vary	Right of jurisdiction	Legislative jurisdiction, judicial jurisdiction, administrative jurisdiction
The legal basis is different	In addition to federal laws, it may be subject to long-arm regulations	Mainly based on federal law
Different legitimacy	May violate international law	Legal

Characteristics of the Long-arm Criminal Jurisdiction

(1) The Principles of Long-arm Criminal Jurisdiction Expand

The United States Court imposing long-arm jurisdiction mark incident was International Shoe Co. v. the State of Washington, 1945 (John, 1980).(International Shoe v.Washing-ton)The decision in the case was a milestone in the formation of long-arm jurisdiction, where the Federal Supreme Court of the United States determined the "principle of minimum connection".Subsequently in Calder v. Jones (1984 (Calder v.Jones, the "effect principle" was born. The doctrine of effect is, " When the act performed by a defendant outside his jurisdiction has consequences or effect upon the court, the court has jurisdiction over that defendant (Yue, & Huang, 2021)." The principles of minimum connection and effect are two basic principles of long-arm jurisdiction on which United States courts govern cases. But the scope of the basic principles is different from the clear characteristics of the specific rules, and the ambiguity of the principles provides more possibilities for expanding interpretation during the application, thus the opportunity to derive other principles.

Principle of intentional acceptance is emerging gradually in the process of the enlargement of the lowest connection principle (Wang, 2008). It became one of the reinforcement principle of minimum contact behavior purpose principle, namely if the defendant in court is better for its own interests, had purpose in the court before engaging in some activity, in the event of a dispute also is willing to solve in the range of the court, where the law can make more benefit, the parties in such a case the case to the court of jurisdiction.

Along with the principle of intentional acceptance is the "principle of predictability".The doctrine was stated in World Volkswagen Co. v. Woodson, 1980 （Word-wide Volkswagen Corp v.Woodson）.It was proposed by the United States court that the exercise of long-arm jurisdiction requires the "foresight" that the defendant may file in court, and the emergence of the principle guarantees the foreseeability, predictability, and accuracy in the application of long-arm jurisdiction (Richard, 1978).

(2) The Legal Basis for Long-arm Criminal Jurisdiction has Increased

The development of long-arm criminal jurisdiction in the information age cannot be separated from the perfect legal system of the United States, especially the legislation in the field of information networks, which provides sufficient legal basis for the development of jurisdiction in the information field. U. S. legislation on information dates back to the Patriot Act's rules on installing telephone surveillance and conducting a thorough investigation of terrorist financing. The United States in the name of opposition and fight against terrorist extremist groups through the Patriot bill, the bill of mobile phone users into the scope of judicial surveillance, citizens' financial credit records, Internet browsing records, communication and chat records has become a monitoring object, and the expansion of the scope of the monitored object will help to realize the great expansion of the power of relevant state organs in the United States.

To deal with cross-border data transfer and a crackdown on crime, the United States has issued the Clear Law on the Legal Use of Foreign Data (hereinafter referred to as the Cloud Act). The bill, on the surface in the name of "public security and global rule of law", demonstrates the US concept of "mutual respect, mutual trust, and joint governance". It forms a unilateral data acquisition institutional framework, providing the opportunity for the United States to legally obtain overseas data." Cloud bill" provides the opportunity of "minimum contact" for the principle of expansion, these "contact" exist in all aspects of the transaction process, from the company listed in the United States to the company operating website using the American server, to the company using the American website, and the settlement process, etc., can become the basis to establish

Vol.3 No.1 2022
https://doi.org/10.37420/j.cer.2022.002

the "minimum contact" (Guo, & Gan, 2000). The Cloud Act makes the institutional barriers to US data from other countries have been largely eliminated and establishes a data collection mechanism to bypass regulatory authorities in countries where data is collected, To substantively extend the effectiveness of law enforcement by some law enforcement agencies to the country where the data is located. For example, Apple iCloud, which previously put data in Guizhou province, still transfers data in the major interests of the US, even if the data entity is not in the United States, and has jurisdiction according to long-arm jurisdiction.

The Current Status of Long-arm Criminal Jurisdiction in the Data Field

Long-arm criminal jurisdiction in the development of the era of big data presents the characteristics of convenience for its expansion, at the same time, the United States take advantage of its field of data, the long arm criminal jurisdiction "minimum contact" based on data, detailed provisions of data jurisdiction, and use their technical advantages to expand jurisdiction, realize the long arm criminal jurisdiction in the field of data further development.

The "Minimum Contact" is Based on the Data

The virtuality of cyberspace gives new opportunities for data development, which provides more basis for the confirmation of the "lowest connection" of long-arm jurisdiction. The "lowest connection" in the "minimum connection principle" is gradually established based on the existence and circulation of data. In " California Software Co. v. Reliable Research Corp, for example, the case is the first case of the "minimum connection" of long-arm criminal jurisdiction. The defendant, in that case, made defamatory statements in Nevada via email and message board system forums, and California courts found themselves entitled to exercise the jurisdiction given the email to California and that the forum could be viewed all online. In that case, the role of the data primarily acted as a "minimum link" of jurisdiction to establish the fact that there was "in-state damage by an out-of-the-state tort."In addition, the California consumer privacy bill (hereinafter referred to as the California act) also takes full advantage of the data, bill scope for business purposes based processing state consumer personal information enterprises, but even if the enterprise is not established in California, is not engaged in-state operations, but when the enterprise stored consumer personal information, or when the enterprise as a third party "share and buy consumer personal information", should accept the jurisdiction of the bill.[6]The Act imposes jurisdiction over content such as consumer personal information as the basis for establishing "minimum links", thus achieving the purpose of expanding the application of the California Act.

Long-arm Criminal Jurisdiction Refines the Regulation in terms of Data Jurisdiction

Data jurisdiction, that is, the jurisdiction formed by the application of national jurisdiction in the field of data, such as personal jurisdiction according to the data-related subjects, and territorial jurisdiction according to the data generation, replication, circulation, etc. From the general trend, the United States standard for determining the minimum connection principle in data jurisdiction is constantly refined, so that the use of long-arm jurisdiction is more targeted, improving the efficiency of the application. Taking the jurisdiction of network data as an example, the judgment standard of the minimum connection principle in this kind of case presents

a reasonable change, transforming from a simple "website access possibility" to a comprehensive judgment mode, and paying more attention to the existence of the substantive connection of the case. In the age of rapid change of network technology, network crime cases more complex, the frequency of such cases increased, in the proportion of the dispute is increasing, so the court in the process of handling such cases constantly practice, explore a more accurate and convenient analysis method, in the practice of many analysis methods, "sliding ruler" analysis method stands out. This method divides the website into passive, active and passive, and active types. Among them, the most common e-commerce websites and other transaction websites in the transaction process mainly show the characteristics of an active type, and this type of website is highly interactive, and it has gradually become the centralized position for a new round of expansion of long-arm criminal jurisdiction.

Data risk Arising from Long-arm Criminal Jurisdiction

Under the trend of the era of big data, cross-border data transfer is common in cross-border services, international trade, and other aspects. Big data is highly praised as "the colorful movement of the third wave"[7], The trend of cross-border data flow has become an international consensus. In the process of cross-border data transfer, the expansion of long-arm criminal jurisdiction in the data field can easily collide with the data sovereignty of other countries, causing interference in the data sovereignty of other countries. In this wave of this era, China is also inevitably facing the data sovereignty risk caused by long-arm criminal jurisdiction.

Inherent Stubborn Disease: There are Loopholes in the Criminal Law Protection of Data Rights

At present, the protection of data sovereignty in China's criminal law is still imperfect. In the process of expanding the long-arm criminal jurisdiction to the data field, this loophole in data protection in China presents great disadvantages, and it cannot calmly cope with the data risks caused by the long-arm criminal jurisdiction. In the process of continuous revision of the criminal law with the development of The Times, the right of data is not protected as an independent legal benefit, but when the data is fixed and recorded to form some information into the category of criminal law protection. In the process of the continuous complexity of information types, China's criminal law brings more information into the scope of protection through revision. The author has sorted out the revision of the information protection content of China's criminal law and reflects through the revision results that the criminal law constantly improves the indirect protection of data rights to a certain extent.

Table 2 The scope of information crimes included in the criminal law sanctions is continuously expanded in the revision process of China's criminal law

Criminal law revision stage	New information crime content
The Criminal Law of 1997	State secrets, information, and other state information crimes are stipulated
	It stipulates that securities trading, trade secrets, insider information, and other public information crimes are committed
1999 Criminal Law Amendment	New futures trading insider information crime

Vol.3 No.1 2022
https://doi.org/10.37420/j.cer.2022.002

The 2001 Criminal Law Amendment (II)	No new
2001 Criminal Law Amendment (III)	New false terrorist information crimes were added
2002 Criminal Law Amendment (IV)	No new
The 2005 Amendment to the Criminal Law (V)	New credit card information crime
The 2006 Amendment to the Criminal Law (VI)	New companies, enterprises of information disclosure crime
2009 Criminal Law Amendment (VII)	New personal information crimes
	Crime of undisclosed information other than new insider information
	New computer information system data crime, here the data refers to the identity authentication information of payment and settlement, securities trading, futures trading, and other online financial services
2009 Criminal Law Amendment (VIII)	No new
The 2015 Amendment to the Criminal Law (IX)	New terrorism and extremist information crimes
	We will expand the scope of personal information crimes
	New illegal information, user information criminal case evidence information crime
	New false danger situation, epidemic situation, disaster situation, and police situation information crimes
	New crimes should not be made public about information
2017 Criminal Law Amendment (X)	No new
Criminal Law Amendment to 2020 (XI)	New information network copyright infringement crime
	Expand the scope of the crime of trade secret information
	New sponsor, safety evaluation, environmental impact assessment, environmental monitoring information crime
	The crime of adding new human genetic resources, the smuggling of human genetic resources and material information
	New gene-editing information crime

However, indirect protection is not the best way to protect data. Due to the difference between the concept of data and information, data carries information, information is a form of data transmission to the receiver, data itself is abstract, and information is according to different receiving purposes, the data processing after forming specific content, so the scope of data is far greater than information.at the present stage, The protection of data rights by protecting specific information is not a long-term solution, Indirect protection methods also cannot fully cover the whole amount of data rights, one side, Data rights are neither independent legal benefits And cannot be attributed to personal interests or property interests and other specific legal interests, Therefore, the appropriate charges may not apply to data infringement cases; on the other hand, The rights to the data for the different subjects are not distinguished, The same data may be presented as different information because of different subjects, The same information is supported by different types of data, That is, there is competition and cooperation between data and information, Data and information are not a one-to-one correspondence. China's criminal law does not classify the data behind the information, the problem between data and information has not been solved, and the provisions on personal data, public data, and national data are vague. In the current situation of insufficient data protection of criminal law, in the case of criminal jurisdiction infringement by long arms, there is no appropriate charge to fully regulate this kind of harmful behavior, which also leads to the lack of criminal law protection of data rights.

New Risks: Criminal Sanctions Undermine Data Regulatory Capabilities

Under the action of the Cloud Act and other laws, the United States can openly obtain the data of some Chinese enterprises, leading to the risk of data leakage. Through criminal sanctions on enterprises, the United States intimidates Chinese enterprises and forms a strong constraint on the development of Chinese enterprises. For example, the U.S. acquisition of ByteDance TikTok's US busines (Zhu, Zhang, & Wu, 2017) In China, TikTok's new CEO Kevin Mayer has publicly said that he will publish the core code used for the company's accounting, and establish the Transparency and Accountability Center to facilitate its review and data practice in the United States. Part of the TikTok data will present a publicly shared state, which challenges both the data security and future development of ByteDance.In addition, in the criminal trial process, China's original data regulatory regulation has been challenged, and Chinese enterprises also have the risk of data leakage. For example, the bank of China branch or subsidiary in the United States as a witness by the US court, with the litigation court, ensure the smooth progress of the case, asked the above branches or subsidiary to provide relevant information, including the bank head office some important data in China, the risk of data leakage in the evidence collection process, but do not cooperate with the evidence may face the American judicial process sanctions, as a witness of bank branches or subsidiaries.

In the process of transnational data transfer, China needs to supervise the data involved in the process of economic transactions and dispute settlements. However, the expansion of long-arm criminal jurisdiction will interfere in economic exchanges and dispute settlement and cause serious interference and damage to China's original data control. Our enterprises listed in the United States or set up branches, products in the production process of American technology and equipment, transnational development using dollar settlement, transactions with American website have become the United States to establish long-arm jurisdiction "minimum contact" key content, so the enterprises also in the long arm jurisdiction coverage, long-arm jurisdiction and our data supervision overlap cause the conflict between regulation, leading to our country data supervision ability is weakened. For example, according to the provisions of the United States in the trading process, overseas enterprises listed in the United States should also disclose some important information to the relevant US departments promptly. In 2014, the US Securities and Exchange Commission (SEC) and Chinese accounting firms were engaged in audit and supervision disputes (Shao, 2021). The United States has accused US-listed Chinese companies of refusing to submit audit drafts, and under China's regulatory rules, accounting firms have no right to provide audit files overseas without permission. The accusation by the United States has damaged China's original data supervision and regulations and disturbed the authority of China's data supervision. In jurisdiction conflicts, the United States can directly protect its overseas branches and subsidiaries under its long-arm jurisdiction, thus avoiding the jurisdiction of other countries. Take Microsoft as an example (Xie, 2000), Microsoft's worldwide operational scale and its monopoly at the technical and data level provide more flexibility for long-arm jurisdiction to facilitate the protection of self-interests through the launch of long-arm jurisdiction. With the expanding principle of the minimum connection, the United States tends to interfere with laws and policies in the handling of cases in other countries on the grounds of "safeguarding domestic information security", violates the case handling system of other countries themselves, and directly interferes in the supervision of other country enterprises on the grounds of information security. For example, the United States adopts a blacklist system for Huawei and other companies. In the absence of relevant evidence that Huawei has violated US law, the United States still blacklisted Huawei on the grounds of information security and human rights, to achieve the purpose of destroying China's data supervision and

Vol.3 No.1 2022
https://doi.org/10.37420/j.cer.2022.002

cracking down on the development of Huawei.

China Responds to the Data Sovereign Risks Brought by Long-arm Criminal Jurisdiction

Data sovereignty is brand new sovereignty in the information era. It is closely related to the country's legal authority, political diplomacy, and economic development. It is the core force based in the international community and also the lifeblood of protecting domestic independence. Given the above data sovereignty risks, China should show innovative measures to safeguard China's data sovereignty by creating legal benefits, expanding the effectiveness outside the criminal law, refining the provisions of the criminal law, improving criminal policies, and learning from off-domain experience.

Clear Data Legal Benefits Through Legislation

As the most severe law, the criminal law itself is not suitable to create a new legal benefit of data rights, but it is suitable to realize the protection of data rights through the form of blank crime and referring to the provisions of data rights and interests in other laws and regulations. In the existing legal provisions in China has not formed a data right protection system, at present, related provisions to the data are scattered in many laws, regulations, and regulations, in the absence of other laws and regulations to define the legal benefit of data rights, there is no reference to the protection of data rights. Therefore, it is urgent to clarify the benefits of data rights through legislation and change the situation of fragmentation and fragmentation of data protection. China should establish the basic law of data sovereignty in the legislation, and clarify the category of data rights in it. The release of the Data Safety Law of the People's Republic of China (Draft) (hereinafter referred to as the Data Safety Law (Draft) indicates that the issue of data security legislation is paying more and more attention. In the future legislative process, data rights should be established as a new legal benefit to provide the basis to protect data rights for the criminal law. In the legislative process, the relevant concepts of data rights should also be clearly defined uniformly, and the existing different norms that define the right of data rights are not unified. The Data Safety Law (Draft) is the starting point of data rights, in the process of the law, should clarify the scope of data rights, data for different storage forms and main body, define data and information, and network concept coincidence and distinguish parts, to avoid different legal concept defects affect the connection of different laws. In the process of data legislation development, minimize the controversial fuzzy definition, timely explain the meaning of the different definitions through legislative technology, clarify the boundaries, and distinguish between the differences. Through legislation, the legal benefits of data rights and the infringement of data sovereignty are clearly defined, to provide a legal reference for the criminal law to protect data sovereignty.

Appropriate Expand the Extraterritorial Effect of Criminal Law

The spatial effect of China's criminal law is realized through the principle of jurisdiction, However, the information age of cross-border transfer of data challenges the existing criminal law jurisdiction in China, The application of the principle of territorial jurisdiction is limited by the virtual space, Unable to determine the location of the crime and other problems in time, For the determined "minimum contact", the website, website, server and so on is also difficult to directly identify as the "location" in the traditional territorial jurisdiction

principle; The principle of human jurisdiction has limits on the nationality of the object under its jurisdiction, The nationality of many virtual subjects is difficult to confirm by using the traditional nationality judgment criteria; The application limitation of the principle of protective jurisdiction limits the scope of its application; The principle of universal jurisdiction over international crime, although without excessive limits on the nationality and crime of the offender, But the principle relies on international treaties regulating the obligations of countries, In the process of growing data sovereignty, International treaties related to data crime in various countries are still constantly improving, So the inadequacy of existing international treaties limits the extraterritorial effect of the criminal law. From the perspective of criminal dispute resolution, although the network security law and the data security law give judicial institutions for external data subject criminal jurisdiction, the data security law only in article 36 clear overseas law enforcement agencies on data stored in our country, for our law enforcement authority are not involved, so referring to the relevant provisions of department law, for extra domain data, the exercise of criminal jurisdiction still need to be based on judicial mutual assistance and cooperation.The expansion of long-arm criminal jurisdiction in the data field challenges traditional jurisdiction. The speed and virtuality of cross-border data flow also make the confirmation of criminal acts and criminal results more difficult, and the existing jurisdiction principles are difficult to apply flexibly to data crime cases. Therefore, it is necessary for China to appropriately expand the off-domain effect of criminal law jurisdiction, and safeguard China's data sovereignty timely and effectively through criminal jurisdiction. For example, expand the scope of territorial jurisdiction and include the data of the acceptance points and issuing points in our country, as well as the data transmitted in the line or network within the territory of the territorial jurisdiction. Enhance the status of the principle of protection jurisdiction, and enhance the application priority of the principle of protection jurisdiction from the legislative level, to realize the timely start of the jurisdiction of China's criminal law in the face of data risks.

Detailed the Provisions of the Criminal Law on the Protection of Data Sovereignty

As mentioned above, data and information do not completely correspond to them, data classification is not equal to information classification, and the protection of different data by criminal law cannot stay at the level of protection of information classification. At the present stage, the information-related charges in China's criminal law cannot contain all kinds of information, let alone the vast majority of the data. The data itself is abstract, and the vague division of the data types will make the data category more chaotic, and the law cannot reasonably classify the data. The classification of data according to different subjects can be roughly divided into three categories: personal data, public data, and national data. Special protection according to different categories is conducive to changing the current situation of insufficient evaluation of the existing criminal law. Personal data for data closely related to the interests of natural persons, such as personal privacy, public data for data involving public interests, such as public security, market order, trade secrets, national data for national security, military secrets, science, and technology. To more comprehensive and reasonable to protect different categories of data, the existing information crime charges should also be rationalization expansion, for more abstract data provide concrete category, the criminal law of information protection of a kind of data, the protection of specific benefits abstract, from the protection of information to protect the data behind the information.

We will Improve the Criminal Policy for Data Sovereignty Protection

Vol.3 No.1 2022
https://doi.org/10.37420/j.cer.2022.002

Current data sovereignty protection criminal policy is still in perfect, for the existing law cannot solve the risk, our country more political means, through diplomatic consultation, for the existing law failed to deal with the risk, most use "one thing", not only in solving the cross-border data flow disputes need to spend a lot of diplomatic resources, and in the face of some virtual network problems cannot be a flexible response, did not form a systematic, strong effect policy prevention early warning means. Therefore, at the level of data sovereignty protection, China should establish a perfect criminal policy for data protection, form the purpose and concept of China in dealing with long-arm criminal jurisdiction, and establish a complete system of normal prevention and event response. Behind the main legislative protection, with the necessary criminal policy to support, the existing law still cannot achieve the performance of the judgment results, through the vacancy of legal means through the principles and purposes of criminal policy, to effectively guarantee the judicial strength. China faces the long-arm criminal jurisdiction system has produced crisis awareness and has taken timely action. When General Secretary Xi Jinping attended the BRICS Summit, he proposed "opposing unilateral sanctions and long-Arm jurisdiction" (The Xinhua News Agency, 2020). In the process of data sovereignty protection in China, we should also adhere to this spirit and hold a negative attitude towards the long-arm jurisdiction in the process of improving the criminal policy.

Learn on International Experience to Improve China's Data Protection

China can draw lessons from international experience to establish treaties and laws, which are suitable and relative to the laws of other countries in practice. In the construction of the legal barrier, China has shown two swords for jurisdiction over long-arm jurisdiction: on September 19, 2020, the Ministry of Commerce promulgated the Provisions on the List of Unreliable Entities (The Xinhua News Agency, 2020). On January 9, 2021, the Ministry of Commerce promulgated the Measures for the Blocking Outside of the Improper Application of Foreign Laws and Measures (hereinafter referred to as the Measures for Blocking). China introduced the Blocking Measures to learn from international experiences, such as the "Block Decree" (Blocking Statute), the laws, regulations of Britain, Canada, Mexico, and Japan against the abuse of long-arm jurisdiction, and corresponding measures. Many experts, scholars, and lawyers pointed out that the core content of China's "blocking measures" is close to the EU's "blocking decree" (Kindu Law Firm, 2021). In recent years, some regulations issued by the EU also comply with the trend of cross-border data transfer and enhance the fight against long-arm criminal jurisdiction, such as the General Data Protection Regulations (GDPR). In the process of building its legal system and policies against long-arm jurisdiction, China should not only learn from EU laws, but also deepen exchanges and cooperation with Europe in various fields, conclude bilateral or multilateral treaties, fully draw lessons from off-domain experience, and form a joint force to counter long-arm jurisdiction.

Conclusion

The evolution and development of long-arm criminal jurisdiction in the United States, the wanton expansion of this jurisdiction in the data field have not to be underestimated, and this expansion caused the risk of data sovereignty affecting the world cannot be ignored. Under the trend of cross-border transfer of big data, China needs to take timely and reasonable countermeasures to combat the hegemony of long-arm criminal jurisdic-

tion in the data field. China is in the rising trend of international competition, the data field is also in the process of continuous exploration and development, long arm criminal jurisdiction in the data field interference will hinder the development of our country data, destroy the existing data supervision in China, so reducing the data sovereign risk brought by long arm criminal jurisdiction is crucial to the development of our country. China can deal with the risks caused by the long-arm criminal jurisdiction of the United States, protect its interests and safeguard the data security in China by creating the legal benefits of data power, expanding the effectiveness, refining the provisions on the data rights of criminal law, improving criminal policies and learning from off-domain experience.

References

John, J. C. (1980). Civil Procedure: cases and materials. *West Academic Publishing*, 1980,65.

Yue, S. M, & Huang, Q. H. (2021). " Long-arm jurisdiction" in International Judicial Assistance and Cooperation and China Response Strategy. *Northern Law*,15 (02),125-136.DOI:10.13893/j.cnki.bffx.2021.02.012.

Wang, S. S. (2008). Long-arm jurisdiction system of the United States courts .Industry economy. *Laws and regulations of Sinopec*, 2008 (10), 31-32.

Richard, H. Field.(1978). "Benjamin Kaplan and Kevin M" Clermont.Material for a Basic Course Civil Procedure.*West Group,* 1978,756—759.

Guo, Y. J., & Gan Yong. (2000). The "long-arm jurisdiction" —— on the reasonableness of establishing jurisdiction in international civil cases .Comparative method study, 2000 (03),266-276.

Qiang, S. G. (2019). Imperial Justice Ararm —— legal support of American economic hegemony. *Cultural aspect,* 2019 (04), 84-93 + 143.

Hu. W. H. (2019). The impact of the US Legal Use of Foreign Data Clear Law on China. *Information Security and Communication confidentiality*, 2019 (07), 30-37.

.Zhu, W. D., Zhang, C.,& Wu, Y. (2017). Big data and the "five-in-one" national strategic application layout .*Mao Zedong Deng Xiaoping Theory Research,* 2017 (03): 8-14 + 108.

Shao, Y. (2021). Network data long-arm jurisdiction —— from "minimum contact" standard to "global management" model.Legal and Business Studies, 2021,38 (06), 73-87.

Xie, W. Y. (2000). Extraterritorial criminal jurisdiction and its implementation.*Law Forum*, (01): 65-69.

The Xinhua News Agency. (2020, November17). *Xi Jinping attended the 12th BRICS Summit and delivered an important speech*.http://www.gov.cn/xinwen/2020-11/17/content_5562138.htm

Department of commerce. (2020, September19). *List of Commerce Order No.4 of 2020.* http://www.gov.cn/gongbao/content/2020/content_5565829.htm

Department of commerce. (2021, January 9). *The Ministry of Commerce ordered No.1 of 2021 to block the improper off-domain application of foreign laws and measures.* http://www.gov.cn/gongbao/content/2021/content_5593445.htm

Kindu Law Firm. (2021, January9). *Interpretation of Blocking the Improper Application of Foreign Laws and Measures*. http://www.gov.cn/gongbao/content/2021/content_5593445.htm

Reincubate. (2018, May25). *General Data Protection Regulations (GDPR)*.http://www.esrf.eu/GDPR