Extraterritorial effect of personal data protection law

Dong Hua Zhou, Jia Wei Liu, Chang Lin Liu, Xiu Juan Li*
School of Law, Anhui University of Finance and Economics, Bengbu233000, China.
* Corresponding Author

Abstract
In the era of data economy, personal data has become an important resource seized by all countries. Under the situation of the extraterritorial expansion and assimilation of the effectiveness of personal information protection laws in various countries and the differentiation of the choice of extraterritorial basis points. Data sovereignty and the "Lotus case" provide the theoretical basis of international law for the extraterritorial effect of personal data protection law; Relying on its own Internet market chips, the EU further expands the extraterritorial effect of the Data Protection Directive in the General Data Protection Regulations, and constructs an EU model based on "place of business standard" and "target orientation standard"; As early as 1998, the United States has applied the extraterritorial effect of the law to cyberspace. In 2018, the California Consumer Privacy Act set the extraterritorial effect of the law based on the principle of effect, and the Clarifying Lawful Overseas Use of Data Act built a "data controller standard" based on its huge number of Internet enterprises, trying to achieve data hegemony. The design of extraterritorial provisions of China's Personal Information Protection Law should learn from the EU "business place standard", objectively type the "target intention standard" to enhance practical application, delete the exhaustive jurisdiction provisions, avoid the ambiguity of legal application, and improve China's foreign-related rule of law system, so as to strive for sufficient voice in the data legislation game.

Keywords
Personal data protection law, extraterritorial effect, target orientation principle, data controller principle.

1. Introduction
"Adhering to the overall promotion of the construction of domestic and foreign legal system" has become the "guiding light" of China's theoretical research on the rule of law since it was established as one of the "eleven insistences" of governing the country according to law. Generally speaking, China has not yet formed a complete and systematic foreign-related legal system; In the field of data, only the personal information protection law (hereinafter referred to as the personal information protection law) initially explores the legislation of extraterritorial effect based on the effect principle. Generally speaking, the effectiveness of public law is restricted by its strict sovereign attribute, and the effectiveness is limited to national territory. Therefore, the research on the extraterritorial effect of domestic law mostly focuses on the fields where foreign-related factors such as antitrust and economic law are obvious, and the extraterritorial effect of personal data legislation is rarely discussed. Take the extraterritorial effect of personal data protection laws in Europe and the United States as the research sample, and put forward countermeasures; Or from the expansion of extraterritorial data jurisdiction in Europe and the United States as the approach, put forward China's coping strategies; From the perspective of the effectiveness
boundary of domestic law, some scholars believe that the basis of extraterritorial jurisdiction over personal information should follow the principle of practical connection. Generally speaking, the above research elaborates how China should "break the situation" in view of the extraterritorial expansion of the effectiveness of other countries' personal data protection laws, but it does not further clarify how to improve the "layout" of the extraterritorial effectiveness of China's personal data protection laws.

On August 20, 2021, the 30th meeting of the Standing Committee of the 13th National People's Congress voted and adopted the personal security law, which was officially implemented on November 1, 2021. It is the first comprehensive legislation for personal data in China. In view of this, this paper analyzes the legitimacy of adding extraterritorial provisions to personal information legislation, takes Europe and the United States as comparative samples, and puts forward the improvement of extraterritorial provisions of China's personal data protection law.

2. Legitimacy analysis of establishing extraterritorial effect of personal data protection law

The so-called data is a way to express information. It is the information content expressed in binary code, which belongs to a part of information. "De anonymization" is the essential difference between the two. It is true that there are still some problems in the academic circles, such as the vague concept and confused use of terms. Extraterritorial effect refers to the effect of a country's authority applying or enforcing its domestic law within its territory, or threatening to apply or enforce its domestic law on acts occurring outside its territory. With the economic globalization, the development of information technology and the change of global governance model, the effectiveness of a country's personal data protection law is increasingly expanding abroad, and the decline trend of legal territorialism in the field of personal data is undoubtedly revealed.

2.1. Data sovereignty requirements

From the perspective of international law, data sovereignty is one of the theoretical sources to determine the extraterritorial effect of personal data protection law. The theory of data sovereignty insists that data governance still belongs to the category of traditional sovereignty. On the one hand, the theory of absolute control over the data flow in the national space is different from the theory of absolute control over the data flow in the international network. Combing the history of national data sovereignty, we can draw a "de sovereignty and then sovereignty evolution trend", that is, the development trend of national data governance from data freedom theory to data sovereignty theory. The theory of data freedom was first derived from the "freedom thesis that cyberspace excludes the interference of sovereign states" put forward by American scholar John Barlow in the declaration of cyber independence. However, this trend has taken a turning point in the follow-up development process. Especially after the exposure of the prism gate incident in 2013, people began to re-examine data sovereignty, talking only about freedom and ignoring the rules of fairness. Its essence is to maintain the existing unfair competition pattern. Data De sovereignty can only aggravate the unfair trend of data flow to developed countries.

2.2. International jurisprudence support

The "Lotus" case in 1927 supported the international jurisprudence of sovereign states to expand the scope of the effectiveness of their domestic law. In addition to the classic argument of whether the French officials have the jurisdiction of criminal cases outside the domestic jurisdiction of the Convention, it has become a criminal case outside the national jurisdiction of France. Just as a scholar believes that it is inappropriate for the court to deny the exclusive jurisdiction of the flag state, It should be recognized that the interpretation meaning of the case
is limited, but so far, the case is the only special case made by the International Court of justice system for national jurisdiction, which opens the debate on the legal logic of national extraterritorial jurisdiction. The Permanent Court of international justice held that "a general rule has not yet been derived from international law, that is, a sovereign state is prohibited from extending the scope of application and jurisdiction of its domestic law to extraterritorial persons, things and acts." In other words, before the formation of international law and international practice that prohibit states from establishing the extraterritorial effect of domestic law, a state has the right to expand the scope of application of domestic law to extraterritorial persons. The conflict caused by the extraterritorial application of domestic law and the response game around the conflict are essentially the process of international law making, because international law is the concentrated embodiment of the will of countries to constantly negotiate and compromise. Any country has the right to judge the creation of jurisdiction rules for extraterritorial people, things or things based on its own interests. Of course, the rationality of this rule needs to be considered by international rules and morality. Further, the extraterritorial effect of domestic law based on reasonable reasons and abiding by the principle of comity has its legitimacy.

The gradual integration of cyberspace and the real space of human activities makes it feasible for national sovereignty to intervene in cyberspace. "We have now entered the era of data 'territory 2.0'. In the current situation that international uniform rules have not been formed, it is a common practice for countries to expand the effectiveness outside the domain through domestic legislation to safeguard national data sovereignty. On the one hand, at the moment when personal data is abused and infringed without restraint, maintaining personal data security is an important topic for all countries. The effectiveness of personal data protection law has a theoretical basis for "touching" extraterritorial reasonably. On the other hand, when the value of personal information is comparable to "oil", for the consideration of national interests, there is a trend of extraterritorial expansion of the effectiveness of legislation in the field of personal information represented by the European Union and the United States.

3. European and American patterns of extraterritorial effect expansion of personal data protection law

3.1. EU situation of extraterritorial effect expansion of personal data protection law

As early as the 1995 Data Protection Directive (hereinafter referred to as the directive), there have been provisions on extraterritorial effects. Article 4.1 (a) of the directive creates the "place of business standard": the data processing behavior occurs in the context of the place of business of the data controller, and the domestic law of the member state is applicable (the place of business of the data controller is required to be located in the EU). This article has become the key connection point of the extraterritorial effect of the directive. In the "weltimmo" case, the European Court of justice threw away the formalistic determination of "business place", which does not require the establishment of legal person or unincorporated institution in the domain, but only requires specific data controllers to have stable arrangements in EU Member States. In the "Google forgetting right" case, the European Court of justice pointed out in its judgment that the data processing behavior of Google search engine for profit is in Google Spain, and the connection between the two cannot be separated. In order to achieve the purpose of applying the directive in cases, it further reduces the "minimum connection principle" in the effect principle.

Although a preliminary attempt has been made in terms of extraterritorial effect, Article 4 is adjusted for Member States to play the role of conflict norms in order to ease and eliminate the legal conflicts of various countries at the level of personal information protection. Under the
framework of the directive, there are some problems, such as inconsistent legislation, decentralized law enforcement, high cost and so on. Moreover, it is not difficult to see from the connection point of extraterritorial effects that, due to the excessive emphasis on "physical connection", the European Court of justice expands the jurisdiction of the directive through interpretation, but it is still limited by the meaning of the terms in the directive itself.

Although a preliminary attempt has been made in terms of extraterritorial effect, Article 4 is adjusted for Member States to play the role of conflict norms in order to ease and eliminate the legal conflicts of various countries at the level of personal information protection. Under the framework of the directive, there are some problems, such as inconsistent legislation, decentralized law enforcement, high cost and so on. Moreover, it is not difficult to see from the connection point of extraterritorial effects that, due to the excessive emphasis on "physical connection", the European Court of justice expands the jurisdiction of the directive through interpretation, but it is still limited by the meaning of the terms in the directive itself.

The general data protection regulation (hereinafter referred to as GDPR), which came into force in May 2018, is the first work of the EU to set extraterritorial effects in the field of personal data based on the principle of effect. On the one hand, while inheriting the business place standard in the directive, GDPR expands the trial scope to the data controller, expands the interpretation of "in the context of carrying out activities" and reduces the "stable arrangement standard". If the non EU business place has an agent in the EU, it may trigger the jurisdiction of GDPR. On the other hand, create a "target oriented standard": "if the data processor or controller does not set up a business place in the EU", this Law applies to the data processing behavior that occurs in the process of providing goods or services to the domestic data subject (no consideration is required) and monitoring the behavior of the data subject in the territory. Using the term "domestic data subject", the data processing behavior of foreigners in temporary transit or temporary residence in the EU may also trigger the application; As for "providing goods or services to domestic data subjects", the preface of GDPR states that online web pages need to be comprehensively judged in combination with the possibility that their language or currency is ordered in the territory of member states or the explicitly mentioned consumers are located in the EU. The European Data Protection Commission has also made a common interpretation of the term "monitoring", including the analysis of the health of data subjects, user portraits and other behaviors. In terms of extraterritorial effect, GDPR has made bold inheritance and innovation to the directive, and further widened the boundary of extraterritorial effect. Facing the introduction of GDPR, US Secretary of Commerce Ross once wrote that "the implementation of GDPR sets unnecessary trade barriers for all countries and regions outside the EU." Some scholars believe that the rule of extraterritorial jurisdiction is only the dream of legislators, but also the nightmare of judges. High standard personal information protection standard belt and broad extraterritorial jurisdiction bring not only high compliance costs, but also uncertain law enforcement and abandonment of the EU market. In essence, this move takes the whole European market as a chip in the international game.

The reason behind this is that one of the reasons for the extraterritorial expansion of EU GDPR effectiveness lies in the basic position of the EU Charter of fundamental rights to include personal information into the protection of basic human rights. After World War II, the EU even took human rights as the core of regional strategy and even global strategy. The German Constitutional Court made it clear in the "first case of population survey" in 1969 that "this is an infringement of personal dignity, even if it is only the preservation of information". Under the framework of the basic human rights protection of personal information in the European Union, the degree of international personal information protection is uneven, and it seems to be due for GDPR to establish a wide range of extraterritorial jurisdiction. Second, in order to unify the data single market and make up for the deficit of the Internet market. In the European e-commerce report in 2021, the population of Europe reached 735 million, which will be twice
the population of the United States, and the proportion of online shopping increased from 60% in 2017 to 73%. The huge population base, perfect network facilities and good online consumption tendency are enough to see the potential temptation of the European market. According to Mary Mikel’s 2019 Internet trend report, among the top 30 Internet companies with the highest market value, the United States holds 18 seats, seven in China and none in the EU. Accordingly, American Internet companies can be said to have firmly grasped the “throat” of the European market, and Amazon has 417 million monthly activities in the UK alone. The huge network service input market is the only remaining advantage of the EU. Article 3 of GDPR aims to protect the interests of personal information subjects and create a fair competitive environment for companies operating in the EU market. Finally, the development of cloud computing technology poses new challenges to territorial jurisdiction. The existing international rules cannot provide sufficient protection for personal data. In this context, the EU intends to seize the voice of global data competition through personal data rights. The “American prism door plan” disclosed by intelligence employee Snowden in June 2013 has attracted the attention of people all over the world. In this grand secret surveillance plan, the United States has been stealing data and information from European and Asian countries. The continuous fermentation of the incident has also become one of the reasons why the safe harbor agreement was invalidated by the European Court of justice. Due to the huge differences in the purpose, methods and standards of personal data protection among countries around the world, the bilateral agreement is essentially the product of compromise and concession between the two sides. The EU GDPR raises the protection standard of personal data, breaks through the jurisdiction of territorialism, relies on the huge Internet market in Europe, requires enterprises to improve their awareness of personal information protection, and aims to influence the world with the EU model before unified national rules and practices are formed.

Despite the controversy, we have to admit that the EU has had an impact on the subjects of international law outside the EU in many legal departments, and has successfully exported the EU’s legal values. Even the United States cannot reach a new compromise with the European Union - the privacy shield agreement in September 2016 after the safe harbor agreement is invalidated. U.S. Internet companies will assume more corporate obligations under the privacy shield agreement. U.S. law enforcement departments can review personal information from the EU only under clear supervision. In this game, the EU is indeed influencing the world with high data protection standards, even if the opponent is the United States.

3.2. American practice of extraterritorial effect expansion of personal data protection law

Compared with the European Union, the United States adopts a decentralized legislative model, and so far no unified personal data legislation has been formed at the federal level. In the field of antitrust law, it is common for the United States to govern foreign entities according to the effectiveness of domestic law. The effect principle was first put forward by the U.S. court in the case of “United States v. American aluminum company” in 1948. The U.S. Federal Circuit Court stressed that the U.S. Antitrust Law can be applied to those monopolistic acts that have a practical impact on U.S. Commerce, without any restrictions on the identity of the perpetrator and the place of implementation of the act. The practice of the United States relying on the extraterritorial effect of domestic laws to exercise jurisdiction over overseas entities can be traced back to the children’s online privacy protection act of the United States in 1998 in the field of personal data. Even if the websites collecting children’s privacy are established outside the United States, they will be regulated by the act. Coincidentally, the children’s online privacy protection act of the United States, which came into force in 2000, also does not require to distinguish between domestic and foreign websites in terms of regulatory subjects. This is the early practice of the United States to combine the extraterritorial effect of domestic law with
cyberspace. The United States has long had legislative practice for the protection of data privacy of special subjects.

The 2018 California Consumer Privacy Act (hereinafter referred to as CCPA) is a U.S. privacy legislation based on GDPR. Firstly, it brings the behavior of having business in California and processing personal data of California residents into the regulation scope of the law. CCPA does not explain what behavior belongs to "having business in California", but reversely stipulates that the law will not apply only when the processing behavior is completely outside the territory of California. Different from GDPR’s definition of the protection subject as all natural persons within the EU, CCPA defines the subject of rights as consumers. According to the California regulation code, consumers should be California tax residents as natural persons, and the term tax residents includes any individual living outside California for the purpose of temporary or short stay but residing in California. The California Consumer Privacy Act breaks through the territorialism, extends the jurisdiction to "processing acts" that have an impact on California outside California, and further takes the personal jurisdiction as the connection point to enhance the scope of application of the law.

A federal act, Clarifying Lawful Overseas Use of Data Act (hereinafter referred to as cloud), signed and entered into force in March 2018, replaces the previous stored Communications Act (hereinafter referred to as SCA) with the data forensics mode of mutual assistance treaty with the standard data forensics mode of data controller. The five-year long "Microsoft Corporation v. the United States of America" was the trigger for the amendment of SCA. In the case, the anti drug authorities of the United States asked Microsoft Corporation to provide the account information of the suspect suspected of drug smuggling. Microsoft Corporation insisted on the "data storage place standard" so that the server storing the data information was located in Ireland and refused to disclose the data, resulting in a fierce conflict with the anti drug authorities of the United States. At the trial stage of the Supreme Court of the United States, the U.S. Congress urgently passed the cloud act, which establishes the "data controller standard" and establishes the obligation of keeping and backing up possession control data for U.S. service providers, and requires that when national security and serious criminal cases are involved, service providers must disclose the data, regardless of whether the data information is stored in the United States or not, The United States puts its personal jurisdiction over data over the territorial jurisdiction of other countries.

Although the United States has not extended the extraterritorial effect of the law to personal data unrelated to the United States, based on the volume and quantity of American enterprises in the global Internet economy, the extraterritorial effect of the law will seriously affect the data sovereignty of other countries. The act also makes it clear that when the user is not a U.S. person or does not live in the United States and the disclosure of the data information violates the laws of foreign governments, the service provider as the data controller can file a reconsideration and refuse to disclose it. When it is against non-U.S. persons and the access to data violates local laws, it is also necessary to decide whether to revoke the disclosure order issued by the U.S. court through comity analysis. Some scholars have pointed out that the application of comity principle in the United States has two characteristics: first, it does not form binding rigid rules; Second, implement the principle of "American interests first", and the "self balancing" mechanism can not really take into account the interests of other countries. With this in mind, the comity analysis procedure of the cloud act is cumbersome and demanding, and the "qualified government" is also judged by the United States. The advantages of the size of the American Internet economy have brought the global data it has into its jurisdiction. At the same time, relying on this condition, the enforceability of cloud is fully guaranteed. According to Google’s transparency report, the passing rate of data call instructions in the United States is as high as 81%, compared with only 7% in Russia.
4. How to improve the extraterritorial effect of China's personal data protection law

Facing the international situation of extraterritorial expansion of the effectiveness of personal data protection laws in various countries, China adheres to the concept of community of network destiny and takes safeguarding data sovereignty as the basic position. Article 3 of the personal security law, which was formally adopted by the Standing Committee of the National People's Congress, officially changed the previous legislative inertia of adhering to territorialism in China. However, in the long run, although China's personal security law combines territorialism with the principle of effect to clarify the extraterritorial effect of the law, it needs to improve the content of the provisions and clarify the application of the provisions.

Design "business place standard" as the connection point of extraterritorial effect, and do technical fuzzy processing on the place where data processing behavior occurs. From the perspective of the design of jurisdiction clauses in the personal security law, China still adopts the territorial jurisdiction thinking centered on the "place where the act occurred". This law is applicable to "data processing behavior occurring in China". However, with the development of cloud technology, the occurrence of data processing behavior is fuzzy and difficult to be used as the "anchor" of jurisdiction. In judicial practice, defining whether the data processing behavior occurs at home or abroad needs to be considered from a more difficult technical level. Refer to the "standard of place of business" of the EU GDPR, and dilute the place of occurrence as the basis of jurisdiction.

Objective typing is the intentional standard of "for the purpose of providing goods or services". On the whole, China's personal security law follows the EU model, Article 3, paragraph 2 (1): "for the purpose of providing products or services to domestic natural persons." It is almost a replica of Article 3.2 (a) of the EU GDPR. The difference is that the EU adopts a more objective data processing behavior that "occurs in the process of providing goods or services to data subjects within the EU". China judges whether it is for the "purpose" of providing goods or services to China, takes the intention of the act as the basis for judging whether it is under the jurisdiction of China, and there is no objective judgment standard to clarify the "purpose". According to the semantic interpretation, all preparatory data processing acts for the purpose of providing goods and services to domestic natural persons should be included in the semantics of paragraph 2 (1) of Article 3. In practice, the judge's subjective judgment of the "intentional standard" is large, which may lead to difficulties in application. In the specific application, it should clarify what behavior belongs to "for the purpose of providing products or services" in the form of judicial interpretation or guiding cases, and deal with it objectively. It is worth mentioning that the "purpose" should belong to the purpose of data processing behavior, not the purpose of the enterprise or enterprise representative.

Revealing the jurisdiction clause is detrimental to the stability of the application of law. Paragraph 2 (3) of Article 3 of China's personal security law stipulates: "other situations stipulated by laws and administrative regulations." The bottom-up provisions sacrifice the stability of the law for the flexibility of application, and apply them to the provisions with extraterritorial effects. At the same time, it also increases the cost of enterprise compliance, which is more likely to further trigger the conflict of jurisdiction between countries. Since April 9, 2020, the Central Committee of the Communist Party of China and the State Council have issued Since the opinions on building a more perfect market-oriented allocation system and mechanism of factors defined data as new production factors. The economic value of personal data as a resource can not be ignored. The fuzzy comprehensive jurisdiction clause may lead to the compliance dilemma of enterprises, which is not conducive to the utilization of personal data resources in China.
5. Conclusion

The extraterritorial expansion of the effectiveness of the personal data protection law is the result of the super regional nature of the network. The development of cloud technology and data transmission technology has blurred the boundary of national sovereignty in cyberspace. The rationality of its expansion has long been based on the theory of international law. Western countries represented by the European Union and the United States have created a relatively complete set of extraterritorial effectiveness systems in their personal data protection laws. The "business place standard" adopted by the EU replaces substantive judgment with formalism; "Target oriented standard" expands the interpretation of the principle of protective jurisdiction. The United States replaced the forensics mode of mutual assistance treaty with the "data controller standard" in the cloud act, which shows the ambition of data hegemony. In terms of the design of the provisions of the personal security law, China can reasonably learn from the EU model, determine the reasonable boundary of extraterritorial effect, and walk out of the road of foreign-related rule of law in line with Chinese characteristics on the basis of respecting the data sovereignty of other countries and taking the principle of International comity as the criterion.

Acknowledgements

"Project* Extraterritorial effect of personal data protection law（No. ACYC2021087）** supported by Graduate Research and Innovation Fund of Anhui University of Finance and Economics.”

References


