TECHNIUM
SOCIAL SCIENCES JOURNAL

Technium.

40/2023

2023

A new decade for social changes

Technium Social Sciences

Powered by PLUS COMMUNICATION
International Communication & PR

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

Legal Approach to International Cooperation on Cloud Storage of Personal Information

Zhang Yi

University of International Business and Economics Law School, Beijing 100029

zoeyzyy@163.com

Abstract. The development of information technology has accelerated the process of globalization and has also internationalized the issue of personal information storage and protection. Personal information can be stored in a cross-border cloud based on the development of Internet technology. However, the separation of the controlling place and the storage place of personal information has brought new challenges to the international regulation of personal information protection. For example, the conflict of legislation, law enforcement, judicial jurisdiction, and the exercise of cyber sovereignty between different countries, etc. In order to strengthen international cooperation on the safety of personal information, it is recommended to promote the sharing of cloud storage of personal information by establishing international self-regulatory organizations, constructing a safety line for the protection of the private rights of information, creating the principle of confirming interests before the usage of information and strengthening the mechanism of punitive compensation in malicious commercial use, etc. It is important to further improve domestic unified legislation and clarify the extraterritorial effects of domestic laws. And introduce data controller standards under the principle of international comity to break the inherent territorial jurisdiction principle. Besides, it is also very necessary to establish and improve the graded and classified management and early warning mechanism for the commercial use of personal information stored abroad. Finally, it is important to take an active part in international negotiations and strive for the right to make international rules on personal information protection.

Keywords. personal information; Cloud storage; International cooperation; Extraterritorial jurisdiction

1、Introduction

As consumers have adjusted to the pandemic lifestyle, the demand for Internet has also become normalized. In recent years, with the explosive growth of massive data, cloud storage, as a new storage method, has become an important technology trend. Domestic companies such as Baidu, Alibaba, and foreign companies such as Apple and Amazon have started to build their own cloud service products. International Data Corporation (IDC) predicts that by 2025, 49% of the world's stored data will reside in a public cloud environment. The Personal Information Protection Law of the People's Republic of China (hereinafter referred to as the "the Personal Information Protection Law"), newly issued in 2021, defines the compliance requirements for "domestic data storage in China". However, it doesn't clarify how to regulate "personal

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

information collected and generated overseas" (such as information directly generated by the consumption overseas).[1]

2、Theoretical and Practical Basis for International Cooperation on Cloud Storage of Personal Information

As the name implies, cloud storage is a storage method based on cloud computing. Specifically, cloud computing technology is used to gather and collaborate the storage pools built by high-speed distributed storage networks to form a safe, convenient, high-speed and low-cost data storage and access system. This kind of distributed storage network often spreads all over the world, which brings conflicts and challenges to the protection of personal information based on network sovereignty of various countries. Personal information refers to all kinds of relevant information that can identify natural persons, and has strong personal attributes. For a long time, the global cooperation in personal information protection has faced great difficulties in practice.[1] Especially with the development of technology and the rapid change in people's lifestyles, personal information such as financial property information, and personal health information, is often exposed. Besides that, countries around the world encounter regulatory challenges in cyberspace, such as network monitoring, network attacks and cyber terrorism. It can be seen that the problems caused by the Internet cannot be completely solved by the power of a single sovereign country, which is more of a problem of global cyberspace governance. However, the protection of personal information, especially the legal protection of personal information stored overseas, varies greatly among countries.[2] Taking the legal practices of the European Union and the United States as examples, the EU emphasizes the protection of personal data privacy and has made clear provisions on the protection of cloud storage of personal information in the General Data Protection Regulation (hereinafter referred to as GDPR), stipulating that "GDPR is applicable to the processing of personal data of individuals in the EU by non-EU organizations, as long as such processing involves monitoring the behavior of these individuals and the processing occurs inside the EU." Even if the personal information is stored overseas, the EU can also exercise jurisdiction over cloud data beyond geographical restrictions. As a country that emphasizes the free flow of data, the United States hopes to achieve its own unilateral global governance by controlling data. The Clarifying Lawful Overseas Use of Data Act in 2018 (hereinafter referred to as CLOUD Act) is a revision and update of the Electronic Communications Privacy Act in 1986, which clearly states that the US government can require US enterprises to provide information located abroad without obtaining court permission or applicable judicial assistance between countries.[2]

[1] Article 40 of the Personal Information Protection Law of the People's Republic of China states that: "Critical information infrastructure operators and the personal information processors that process the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity shall store domestically the personal information collected and generated within the territory of the People's Republic of China. Where it is truly necessary to provide the information to an overseas recipient, the security assessment organized by the national cyberspace administration shall be passed. Where laws, administrative regulations, or provisions issued by the national cyberspace administration provide that security assessment is not required, such provisions shall prevail."

[2] Article 4 of the Personal Information Protection Law of the People's Republic of China states that: "'Personal information' means all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized."

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

3、The Dilemma of International Legal Cooperation on Cloud Storage of Personal Information

The conflict of jurisdiction

In the field of international law, the distribution of jurisdiction among States is a very important issue. For example, GDPR regulates the data processing behavior of business institutions inside the region based on Data Protection Directive in 1995 (hereinafter referred to as DPD). Article 4 (1) of DPD involves two criteria: (1) Does the controller have a "business organization" in the territory of the EU member states? (2) Has personal data been processed within the scope of the business organization's activities? If the above two conditions are met at the same time, it should be applied to DPD, regardless of whether such data processing behavior occurs within or outside the European Economic Area (hereinafter referred to as EEA). The location of data or the physical operation of data is not decisive.[3] Such jurisdiction has actually broken through the territorial principle and has had an effect on cloud data located outside the country. In order to cope with the extraterritorial jurisdiction of the European Union, the United States reached an agreement with the EU in 1998 and established a self-regulatory system that allowed American enterprises to participate in the "Safe Harbor" program to ensure that American enterprises, including cloud providers, can import commercial personal data from the EU. In February 2016, the United States Department of Commerce and the European Commission reagreed on a data transfer framework known as the "Shield of Privacy".[4] At the same time, the CLOUD Act was also formulated, which stipulated the principle of data globalization. The expansion of extraterritorial effects of domestic data jurisdiction implied by these legislative changes also means that exercising jurisdiction based on territorial sovereignty can no longer meet the needs of personal information protection in the international field in the cloud era.[3]

The exercise of network sovereignty

The competition among big countries has intensified the conflicts in the global cyberspace and also brought new challenges to the legal protection and international cooperation of personal information. As one of the permanent members of the United Nations, China has always played an active role in cyberspace cooperation. As early as 2011, China, Russia, Tajikistan and Uzbekistan, as members of Shanghai Cooperation Organization, jointly submitted the International Code of Conduct on Information Security to the 66th General Assembly of the United Nations, aiming to strengthen international cooperation to address common challenges in the field of information security. In 2016, China issued the Cyber Security Law of the People's Republic of China, which clearly defined the purpose of safeguarding cyberspace sovereignty and proposed the information protection requirements for "security assessment" of domestic data outbound.[4]

The EU has continuously introduced laws and strategies on cyber security in recent years, proposing "digital sovereignty" and "technological sovereignty" to strengthen cyber

[3] See "EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield" on European Commission, available at http://europa.eu/rapid/press-release_IP-16-216_en.htm, February 2, 2016.

[4] Article 37 of the Personal Information Protection Law of the People's Republic of China states that: "Where organizations that are authorized by laws and regulations to exercise the power of administering public affairs process personal information to fulfill their statutory functions, the provisions of this Law on the processing of personal information by state organs shall apply."

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

security governance. Since the Snowden incident, the EU cyber security strategy has changed from passive defense to active one, by constantly improving the top-level design, unifying laws and standards, exercising cyberspace sovereignty through data security supervision and creating a "three in one" cyberspace security system.[5] At the same time, the United States pursues a strategic tendency of super sovereignty. Its advocacy of "network freedom" has a distinct double standard. It advocates "the United States first" for matters involving its own interests. This kind of unilateral governance is very obvious in the cloud space lacking geographical boundary restrictions.

The practice of the EU and the United States in safeguarding and even expanding their own network sovereignty also represents a trend of sovereign exercise of countries in the international network society. It is an inevitable trend under the background of economic globalization, which also brings new issues and challenges to the power division and cooperation of countries around the world in the exercise of network sovereignty.[6]

The distribution of rule-making power in cyberspace

Some countries and international organizations have formulated their own rules to regulate the protection of personal information stored in extraterritorial space. For example, the Guidelines for Privacy Protection and Cross border Flow of Personal Data, first issued by the Organization for Economic Cooperation and Development (hereinafter referred to as OECD) in 1980, set eight basic principles for the cross-border flow of personal data. In 1990, the United Nations issued the Guidelines for the Regulation of Computerized Personal Data Flies, which is more open to cross-border data. In 2013, OECD made a comprehensive revision to the 1980 Guidelines, further emphasizing that data controllers need to be responsible for the personal data they control, regardless of where the data is stored. In the same year, the Asia Pacific Economic Cooperation (hereinafter referred to as APEC) adopted the Cross-border Privacy Rules System, requiring that "governments should ensure that there are no unreasonable barriers to cross-border data transmission, and at the same time, they should cooperate with foreign governments to protect the privacy and security of their citizens' personal information at home and abroad."[7] It can be seen that most sovereign countries in the international community are actively promoting win-win cooperation in cyberspace through negotiation and consultation. However, with the deepening of cooperation, the competition of the rule-making power in cyberspace has become increasingly fierce. It is a new round of rule-making game under the background of international community connectivity. The country that can take the lead in rule-making in this field will be able to take the lead in information protection, storage, commercial utilization and other aspects in the future development for a long period of time, so as to provide guarantee and support for the development of other areas of the country in cyberspace.

The strength of a country's protection for cloud personal information is closely related to its rule-making power in international cyberspace. Taking the United States as an example, the United States has always held a major voice in APEC. In the field of investment, the United States has successively passed Foreign Investment and National Security Act, and Foreign Investment Risk Review Modernization Act, giving the committee the right to review investments that "maintain and collect personal sensitive information of American citizens." In addition, the United States has further consolidated its extraterritorial jurisdiction through the "sufficient connection" standard.[8] In fact, the United States has incorporated the fight for the right to speak in cyberspace into its territory of pursuing "unilateralism governance", trying to strengthen its restriction on the information field of other countries by controlling cyberspace in the global scope. With the rapid development of information technology, international

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

competition in modern society has evolved into the competition of the power of information and rule-making between different countries.

4、Legal Approach to International Cooperation on Cloud Storage of Personal Information

Promote the sharing of cloud storage in cyberspace on the premise of national sovereignty

The principle of national sovereignty is an important cornerstone of modern international law established by the Charter of the United Nations. As a new type of space, cyberspace is the fifth largest space for human activities after global public areas such as ocean space, outer space and polar space. As for the information in virtual cloud space, it is important to actively promote the sharing of it on the basis of the network sovereignty of various countries.[9]

First of all, an International Self-regulatory Organization on the security of personal information storage should be established. At present, the member countries of the global Internet institutions are mainly western developed countries represented by the United States and the institutions have become their tools to promote unilateralism and network hegemony.[5] An international cloud storage governance organization with equal participation should be established. The Self-regulatory Organization should be located at an international non-governmental organization, allowing influential enterprises from all over the world to join as members and providing technical support and standards for information sharing. The International Self-discipline for the Cloud Storage of Personal Information should be formulated to reach an international consensus on general guidance concerning the collection and management of personal information, such as the access qualification of cloud service providers, operation standards for key information infrastructure, and emergency response mechanism of personal information security.[10] It should clearly stipulate the self-discipline rules that all members should abide by and emphasize that industry self-discipline should be combined with the rule of law to build an international self-discipline system in the Internet field.

Secondly, a security line for the rights in the protection of personal information should be constructed. The Personal Information Protection Law and the Data Security Law of the People's Republic of China, which were issued successively in 2021, clearly emphasized the requirements for bottom-line protection of personal information.[6] But it is all-too-simple and conceptual fuzzy in regulating personal data. The concept of "business ethics", "social

[5] The global Internet system is mainly composed of the Internet Corporation for Assigned Names and Numbers (ICANN), five Regional Internet Registries (RIRs), the Internet Society (ISOC), the Internet Architecture Board (IAB), the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), the International Organization for Standardization (ISO), the World Wide Web Consortium (W3C). Several international organizations mainly provide operational services, technical support, policy support and other functional services.

[6] Article 2 of Data Security Law of the People's Republic of China clearly states that: "This Law shall apply to data processing activities and the security supervision thereof conducted in the territory of the People's Republic of China. Those that conduct data processing activities outside the territory of the People's Republic of China to the detriment of the national security, public interest, or lawful rights and interests of citizens and organizations of the People's Republic of China shall be held legally liable in accordance with the law."
Article 10 of the Personal Information Protection Law also further emphasizes: "No organization or individual may illegally collect, use, process, or transmit the personal information of another person or illegally buy or sell, provide, or disclose the personal information of another person; or engage in personal information processing activities compromising national security or public interests."

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

morality" and "social responsibility" are not clearly defined, leaving room for discretion in the bottom-line protection of personal information. Inadequate principled provisions of domestic laws also lead to inadequate protection of personal information in the space of international law.[7] With the development of information technology, personal information has become increasingly commercialized after being stored and processed. Even the data processed and stored overseas is also the property of citizens. Therefore, the storage and use of personal information related to personal health, family and other personal dignities must be carried out for legitimate purposes. And fundamental rights should be clearly included in self-discipline, such as the right to know, inquire, correct, delete, etc. These fundamental rights should be explicitly incorporated into international conventions, allowing citizens to have international rights relief when their basic rights are violated.[11]

Finally, the principle of benefit recognition before the use of personal information and the mechanism of punitive compensation for malicious commercial use should be established. In order to balance the protection of personal interests and the efficiency of commercial transactions, provisions on the convenience of market transactions in accordance with the principle of interest recognition should be established. For example, when personal information is stored in the cloud, the users should make a commitment in advance to the general use of some of the common information, and put forward a prior request for strengthening the defensive protection of the part involving personal sensitive information. For those who use personal sensitive information for profit or illegally use personal information in violation of legal provisions and personal will, the corresponding punitive compensation mechanism should be clarified. In addition to compensating for the corresponding losses, the cloud service provider may be restricted or even banned from engaging in the related cloud business for a certain period of time as a way to strengthen the deterrence of malicious use of personal information.[12]

Clarify the extraterritorial effect of domestic laws

The core issue of international cyberspace governance is the legal regime. In the era of the digital economy, only the rule of law can truly strengthen the safety of personal information protection. In the international community, countries are accelerating the pace of legislation related to information protection. By 2021, more than 140 countries have introduced relevant rules for data security protection.[8] China has also promulgated relevant laws and regulations for personal information protection. For example, the Cyber Security Law of the People's Republic of China issued in November 2016 and the Measures for the Evaluation of the Exit Security of Personal Information and Important Data (Draft for Comments) issued in April 2017 have both stipulated the domestic supervision of personal information.[13] However, even the Personal Information Protection Law newly issued in November 2021 does not make specific and

[7] For example, Article 12 of the Universal Declaration of Human Rights adopted by the United Nations in 1948 stipulates that everyone should be protected from the interference has the right to legal protection and inviolability of his private life, family, residence and communication. The personal information of citizens, especially the personal information related to their health, family, residence and consumption, is an important part of their personal privacy.

[8] In the process of legalization of information protection, the protection of personal data has gradually become the focus, and more than 80 countries have introduced relevant laws to protect personal privacy data. In 2020, Singapore revised the Personal Data Protection Act (PDPA), Japan revised the Personal Information Protection Act (APPI), Australia, the Netherlands, South Korea and other developed countries have also promulgated and implemented laws to protect personal privacy data, and have successively revised relevant laws according to the needs of the continuous development of the digital economy.

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

targeted provisions on the protection rules of personal information stored overseas through the cloud.

On one hand, it is important to further clarify the extraterritorial effects of domestic laws. The data controller standard can be introduced to break the inherent territorial jurisdiction, as well as following the principle of international comity. The expression of "data processor" in the Personal Information Protection Law is very similar to the expression of "data controller" under the GDPR. So the meaning of the "data controller" standard in China's domestic law can be further defined by referring to the Guidelines on the concepts of controller and processor in the GDPR version for public consultation raised by the European Data Protection Board. Firstly, the type of data controller should not be strictly limited. It can be natural persons, legal persons, public authorities, institutions or other entities, but generally, it is an organization, not including individuals within the organization (such as employees or board members);[14] Secondly, the right of the data controller should be derived from formal laws and regulations; Finally, in terms of substance, the controller should have the right to determine the purpose and method of data processing (why and how to process data), the scope of data collection, the range of data involved and the right to determine the retention period of personal data. If the above formal and substantive identification criteria are met at the same time, it can be identified as the data controller. On this basis, as long as the actual data controller is a Chinese company, even if the data is stored in a cloud server outside China, that data controller should cooperate with Chinese government to obtain the data.

On the other hand, it is necessary to improve the hierarchical and classified management mechanism for the commercial use of overseas personal information. First of all, access management should be carried out for cloud service providers. As for cloud service providers with overseas data centers and infrastructures, special cloud business licenses could only be issued after security assessment by relevant authorities; Secondly, differentiated management should be carried out in cloud storage. As for the information that has been disclosed according to law, it can be disclosed to the data controllers which are legally established in China. However, as for overseas data controllers, due diligence and risk assessment should be conducted before data disclosure.[15] Finally, it is necessary to improve the risk prevention mechanism and strengthen the security technology guarantee. This mainly involves the specification of the information security guarantee obligations of cloud service providers. The overseas business of cloud service providers should be supervised in a full process. At the preliminary stage of concluding the service contract, cloud service providers should be prohibited from exempting themselves from responsibilities in terms of information security assurance by using standard terms, and the obligations of security and confidentiality should be the mandatory provisions of the contract. At the same time, a special dispute resolution center should be set up. In view of the fact that the compensation for contract damages is generally limited to the direct losses of users, and the current cloud service costs are almost at the level of "ultra-low or zero". Once the cloud service provider infringes the users' rights due to its fault, the users cannot get reasonable compensation. The minimum compensation limit of cloud service providers should be specified to protect the basic rights and interests of users whose personal information has been damaged.[16]

Actively participate in international negotiations

The dispute over personal information protection standards has never been the origin of legal conflicts between countries. The issue of "social dumping", which has attracted the attention of the international community before, and the setting of human rights clauses in trade

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

agreements have triggered a strong response from the international community.[17] The root is not whether a country has the right to implement certain legal standards in its own country, but whether the implementation of such standards can achieve the policy goals expected by the country. Therefore, the legal protection of overseas cloud data is, to a certain extent, subject to the recognition of a country in international rule-making, which is closely related to the rule-making power of a country.

On one hand, China should actively join the soft law system of personal data protection. The regulations on personal information protection in the international community can be divided into three historical stages.[18] The first stage mainly focuses on the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued by the OECD in 1980 (hereinafter referred to as OECD Guidelines) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. The second stage is represented by the DPD in 1995. The third generation is the GDPR which came into force in 2018. However, China has not yet joined the influential international soft law system on data privacy protection, such as the aforementioned OECD Guidelines and the Global Cross Border Privacy Rules (hereinafter referred to as CBPR) under the 2012 APEC Privacy Framework. The CBPR is jointly participated by privacy enforcement agencies, accountability agencies and enterprises, which forms a strong substantive constraint on enterprises. As a multilateral mechanism, the implementation of the CBPR depends on the strict enforcement of the domestic privacy agencies, which accelerates the pace of domestic legislation to protect personal data privacy. China should actively join the international soft law system represented by the CBPR. Cyberspace Administration of China could be designated as the privacy enforcement agency according to the requirements of the rules and assume the functions of information sharing, joint investigation and law enforcement.[19]

On the other hand, China should expand the legitimacy space of its domestic laws in bilateral or multilateral treaties. First, both parties' rights, obligations and responsibilities should be clearly stipulated in bilateral treaties on issues involving the storage and protection of overseas personal information. For example, both parties should equally protect the personal information stored in the other country based on national treatment and provide timely relief when the personal information is maliciously used by a third party. Second, in terms of the exercise of extraterritorial jurisdiction of law enforcement, an overseas data protection mechanism could be established, including information sharing, convenient delivery of documents, joint investigation, etc.[20] At the same time, the principle of proportionality can be introduced to limit the extraterritorial data jurisdiction of the contracting parties, as well as reasonably determining the exercise boundary of the right to extraterritorial protection of personal information storage. Thirdly, it is necessary to clarify the legitimacy of domestic laws under the Free Trade Agreement (hereinafter referred to as FTA) and other regional agreements. Article 38 of the Personal Information Protection Law clearly stipulates the conditions that should be met to provide information overseas: "security assessment by Cyberspace Administration of China", "certification by professional institutions", "standard contracts signed with overseas receivers", etc. However, paragraph 2 of this Article provides an exception to the standards concluded by China, which means that although China has the right to prohibit cross-border storage that does not meet China's data protection standards, this standard is subject to the exception exclusion of "international treaties and agreements". China should not only protect the extraterritorial storage and circulation of personal information by domestic legislation, but also actively promote the further incorporation of such protection measures and standards into regional agreements such as FTAs. A connection should be built between

domestic standards and international mechanisms, giving consideration to the balance of interests between data localization and the free flow of data.[21]

5、Conclusion

The emergence of cloud computing has accelerated the formation of cloud storage of personal information. At the same time, it also brings new challenges to domestic legislation and international cooperation in personal information protection. Personal information is often processed into data property with strong commercial attributes, which is of great significance to a country's economic and trade development. Therefore, both developed and developing countries try to compete for governance in international cyberspace. There are often jurisdictional conflicts for personal information stored in the cloud of different countries that have broken through geographical restrictions. Especially after the Snowden incident, network sovereignty security has become an increasingly controversial topic in the international community. This paper tries to promote the sharing of cloud data in international cyberspace on the premise of network sovereignty. Through the establishment of an International Self-regulatory Organization on the security of personal information storage and the combination of industrial self-regulation and rule of law, an international self-regulatory system could be built in cyberspace. The core of governance in international cyberspace is a legal issue. While improving domestic legislative protection, China should actively promote win-win cooperation in cyberspace through negotiation and consultation, build a connection between domestic standards and international mechanisms, balance the interests between data localization and free data flow, and enhance China's power of discourse in the formulation of international digital trade rules. International cyberspace governance needs to be based on the rule of law. In the face of the reattack of the anti-globalization trend, adhering to international cooperation not only reflects China's responsibility as a major country, but also conforms to the basic concept of a human community with a shared future in cyberspace.[22] The construction of a community with a shared future in cyberspace cannot be separated from the improvement of national standards, and more importantly, it needs to rely on the consensus reached by all countries on cyberspace governance on the basis of consultation and negotiation. The internet was never intended to be a homogeneous, borderless virtual space. It is, and was designed to be, a network of networks. China should take an active part in building an international conference platform to show the interests of developing countries to the international community, and advocate the establishment of an international legal cyberspace. On the premise of rule of law, a system for the international protection of personal information should be established to further promote the construction of a community of shared future in cyberspace.

References

[1] Mirzet S. Ramich, Danil A. Piskunov. The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes [J]. Vestnik RUDN International Relations, 2022 (02): 238-255.
[2] Dove, Edward S. The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era [J]. The Journal of Law, Medicine & Ethics, 2018 (04): 158-162.
[3] Brian Simpson, Maria Murphy. Cyber-privacy or Cyber-Surveillance? Legal Responses to Fear in Cyberspace [J]. Information & Communications Technology Law, 2014 (03): 189-191.
[4] Yao Wenbin, Han Si, Li Xiaoyong. Security Sharing Scheme for Encrypted Data in Cloud Storage [J]. Journal on Communications, 2015 (10): 211-218.

Technium Social Sciences Journal
Vol. 40, 156-165, February, 2023
ISSN: 2668-7798
www.techniumscience.com

[5] Daniel S. Hoops. Lost in Cyberspace: Navigating the Legal Issues of E-Commerce [J]. Journal of Electronic Commerce in Organizations, 2012 (01): 35-42.
[6] Wang Xue, Shi Wei. Expansion of Extraterritorial Jurisdiction over Personal Data and the Construction of China's Enterprising Path [J]. Henan Social Sciences, 2022 (05): 61-67.
[7] Biljana Karovska-Andonovska, Nenad Taneski. Legal Aspects of Security in Cyberspace [J]. Bezbednosni Dijalozi, 2020 (01): 99-102.
[8] Shao Zhuli. International Coordination of Personal Information Protection [J]. Wuling Academic Journal, 2017 (01): 87-92.
[9] W. Kuan Hon, Julia Hörnle, Christopher Millard. Data Protection Jurisdiction and Cloud Computing-When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing [J]. International Review of Law, Computers & Technology, 2012 (02-03): 129-132.
[10] Y. Tony Yang, Erin Grinshteyn. Safer Cyberspace Through Legal Intervention: A Comparative Review of Cyberbullying Legislation Safer Cyberspace Through Laws [J]. World Medical and Health Policy, 2016 (04): 460-477.
[11] Olufunmilayo B Arewa. Securities Regulation of Private Offerings in the Cyberspace Era: Legal Translation [J]. The University of Toledo Law Review, 2006 (02): 331-335.
[12] Shao Yi. Unilateral Expansion of Extraterritorial Data Enforcement Jurisdiction [J]. Social Science, 2020 (10): 128-129.
[13] Christopher Millard. Cloud Computing Law [M]. Oxford University Press, 2013.
[14] Zhu Depei. Data Localization in the Context of "Deglobalization" [J]. Journal of Henan Institute of Technology, 2020 (05): 69-72.
[15] Zhao Hongrui, Li Shuming. International Governance of Cyberspace: Status Quo, Prediction and Response [J]. Guangxi Social Sciences, 2021 (11): 109.
[16] Charles J. Jr. Dunlap. Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors [J]. Nebraska Law Review, 2009 (03): 712-713.
[17] Li Yan. The Analytical Method, Framework and Significance of the International Governance Mechanism of Cyberspace [J]. Information Security and Confidentiality of Communications, 2019 (09): 38-45.
[18] Francoise Gilbert. Cloud Service Contracts May be Fluffy: Selected Legal Issues to Consider before Taking off [J]. Journal of Internet Law, 2010 (06): 1-3.
[19] Ren Ying, Li Huawei, Wang Lina. A New Data Collaboration Service Based on Cloud Computing Security [J]. Materials Science and Engineering, 2017 (01): 1-7.
[20] Zhao Haile. Personal Information Protection International Legal Conflict and Countermeasures from the Perspective of Data Sovereignty [J]. Contemporary Law, 2022 (04): 87.
[21] I Trotter Hardy. The Proper Legal Regime for "Cyberspace" [J]. University of Pittsburgh Law Review, 1994 (04): 993-995.
[22] William D. Bryant. International Conflict and Cyberspace Superiority: Theory and Practice [M]. Scopus, 2015.

About the author: Zhang Yi, female, Zhengzhou, Henan Province, studied as a doctor in the School of Law of the University of International Business and Economics, an assistant of Internet Finance Law Research Center of the University of International Business and Economics, with the main research field of economic law. No. 10, Huixin East Street, Chaoyang District, Beijing, 18810656852, Email: zoeyzyy@163.com.