Advances in Social Science, Education and Humanities Research, volume 554
Proceedings of the 7th International Conference on Humanities and Social Science Research (ICHSSR 2021)

International Law Thinking on Data Security In TikTok Incident

Haokun Niu[1]，Jiahui Hong[1]*

[1]*School of China University of Geosciences, Wuhan, Hubei, China 430074*
**Corresponding author. Email: ishongjhcug@gmail.com*

ABSTRACT
National data security is playing an increasingly important role in the development of a country. Nowadays, it's universally acknowledged that cooperation should be strengthened in the international arena to safeguard international data sovereignty security. Transnational applications will inevitably bear the risk of being sanctioned due to conflicts between countries. The plight of TIKTOK in the United States fully demonstrates the international risks faced by transnational applications, so this work will focus on the conflict between data utilization and national security and privacy protection. Taking TikTok as an introduction, under the environment of globalization, some countries taking national force to blockade, implementing data locality of data flow, is committed to building data circulation "centralized" behavior also do not have merit, through look up corresponding conventions, in an effort to fully protect the voice in the field of information data, improve the data flow rule.

Keywords: *Ban promulgation, Data flow, National Information security, Data network order*

1. INTRODUCTION

In July this year, the United States in the trump of the government's support, and promote to citizens' personal information, the data reveal that "threat to national security", citing the TikTok has adopted a series of measures ,such as threat warning, trade terms and ban trading terms and etc. On July 31, said trump, unless sold in the United States business agreement, otherwise TikTok will be forced to shut down its business in the United States before September 15. On July 20, the U.S. house of representatives passed a bill. On July 22, the SENATE Homeland Security and Governmental Affairs Committee voted unanimously to ban the use of TikTok on federal government devices. By July 31, Trump said he would ban TikTok from operating in the United States, citing national information security for other mobile phone app is disabled, the United States is not the first, after have such as India [India's electronics and information technology (miit) said, according to the country's policy of the information technology act and related laws and regulations, decided to disable 59 applications, these applications is engaged in the activities of "damage" India's sovereignty and the integrity of India, defense, national security and public order. The department claimed that it received complaints from various channels, according to the above application is data security and privacy concerns. These applications on mobile or mobile devices will be disabled.]59 Chinese softwares, including WeChat and TikTok, are prohibited from being used in India on the grounds that "the activities these apps engage in are detrimental to India's sovereignty and integrity, national defense, national security and public order"; Since then, Countries such as Australia and Japan have also begun "close" surveillance of TikTok. Basically, the national security maintained by all countries requires the survival and development of sovereign states to be inviolable and unthreatened. The consensus and practice of the international community also believe that safeguarding national security is also a fundamental right granted to sovereign states by international law. However, due to the globalization of data network, the interests of other countries will inevitably be touched in the process of safeguarding information security. The principle of sovereign equality established in the Charter of the United Nations in 1945 covers all fields of exchanges between states parties, and its principles and spirit should also be applied in the information network space. Therefore, measures taken by a country to safeguard its information security should not only be based on domestic law, but also be adjusted by international law.

2. DISCUSSION ON THE ILLEGALITY OF ISSUING A BAN ON THE GROUNDS OF NATIONAL SECURITY

2.1. It Undermines the Protection of Individual Rights under International Human Rights Law

Respect for international rules and international law is a prerequisite, despite differences in national policies. The security of citizens' personal information and the possession of personal privacy data are citizens' individual rights, and the protection of personal privacy is also the requirement to realize the protection of human rights. Network operators in the user data security has corresponding protection obligations [including to obtain user consent, users have the right to be forgotten, have the right to correct and so on a variety of rights.], citizens also have free access to applications. After the ban, citizens' free use of apps was restricted. In the universal declaration of human rights,"anyone's personal life, family, home and communications shall not be any interference, shall be subjected to attack his honour and reputation. Everyone has the right to enjoy legal protection, so as to avoid such interference or attacks."[1-3]As what is stipulated in article 19: everyone has the right to claim and the freedom of opinion; this right shall include freedom to hold claim without interference, and through any media and regardless of national borders to seek, receive and send messages, and the freedom of thought. Paragraph 1 of article 27:"Everyone has the right to participate freely in the cultural life of society, to enjoy the arts and to share in the progress of science and its benefits." The Universal Declaration of Human Rights " No person shall be arbitrarily deprived of his or her property. "It also provides for the protection of citizens' private property security. Therefore, the United States' administrative sanctions on the grounds of national security are a violation of citizens' individual rights, [4,5]and it also fails to fulfill the obligation of safeguarding citizens' individual rights in national law.

2.2. It Violates the WTO Principles of Openness, Transparency and Non-discrimination

The United States has been a representative of the free flow of data. In 2013, the United States, Australia, Canada, European Union and other 23 members based on GATS trade under the WTO Agreement of the international service trade Agreement (Trade in Services Agreement, hereinafter referred to as TISA), the United States require "member service provider the government can't prevent another member, the transmission, access, treatment, storage information from within its borders or other countries." There are no exceptions to this clause. From the perspective of relevant WTO regulations, the double standards demonstrated by the US in allowing cross-border data flow and the sanctions against TikTok are contrary to the principles of market economy, and even more contrary to the principles of openness, transparency and non-discrimination that the WTO has been striving to achieve.[1,2,6].

2.3. The Expropriation of Data Property Lacks Treaty Support

After the promulgation of "TIKTOK", a series of executive orders implemented by the US government relying on public power have constituted indirect expropriation of "TIKTOK" from a practical point of view. Whether the administrative order requires data processing will lead to indirect expropriation of enterprise data property is also a new theoretical issue.

Therefore, data property is an inevitable trend of international development. Recognition of TIKTOK's data property in an executive order issued by the White House. The "interests and rights" of Bytedancing's section 2 (b) (II) requirement to divest include "any data acquired or derived from users of the TIKTOK application or Musical.ly application in the United States.". In addition, the executive order requires Bytedance to certify in writing to CFIUS that it has destroyed all data and copies required to be stripped under Section 2 (b) (ii), and to require an audit. Since the administrative order has recognized the interests and rights of data, the provisions of data destruction required in the administrative order are most likely to be unreasonable interference in the use, possession and disposal of data property, which constitutes indirect expropriation.[7,8]Based on theoretical analysis, however, due to the lack of relevant treaties between China and the problem of data protection, also did not undertake the international arbitration rules of the problem, in fact for data can be as a collection of objects and the citizen right of privacy behind hidden in the data, information security is also need relevant provisions of the relief, also need to be regulated treaty.

3. HINDER THE ESTABLISHMENT OF INTERNATIONAL DATA PROTECTION SYSTEM

3.1. Practical Obstacles to International Data Protection

Cyber information security, which endangers individual privacy, national security, economic lifeline and social stability, is playing an increasingly important role in a country's comprehensive strength. With the increasingly fierce international competition in the field of information technology, countries pay more and more attention to information security. Cross-border data flows freely to give adequate space to multinational companies use data, and achieve privacy depend on countries to establish a good system of data protection, countries need

to strengthen the autonomy of data protection to ensure national security, the privacy protection inevitably hindered the data flow freely, it reflects a fundamental contradiction problems. Legal analysis of the "Tik Tok" Incident -- also on the Improvement of international economic and Trade rules for data Utilization, author Ding Jingwen talks about the fundamental contradiction between the freedom of data flow and national security and privacy protection, which is known as the "three difficult choices" in academic circles.[4,5,8].

Through analysis, it is not difficult to conclude that the relevant rules of data utilization in the modern international community are not complete, and were once destroyed due to improper actions of some countries. The free flow of cross-domain data in data utilization is very likely to cause national security problems in international trade, and it is precisely because the trade of transnational corporations has caused the destruction of the order of international data network.[9]The "Tik Tok" incident also reflects that there is no clear legal rule in international law on the relationship between data utilization and national security, and there is a blank space. Some countries, represented by the United States, encourage the free flow of data across river basins internationally. They want to promote the development of their own enterprises by collecting data from other countries, but restrict the use of data for the sake of national security at home. This is obviously unfair and undermines the order of the international data network.

3.2. National Data and Information Security Maintenance without International Standards

Cyberspace knows no boundaries. Every country is a member of this space. In retrospect, most of the incidents related to network information security have international characteristics. In such an era of information explosion, network information security involves politics, economy, military, daily life and other fields, involving a very wide range of issues, but also more complex, it is probably difficult for a country to respond calmly.

Table 1. The International Convention of Data Security

Signing time	Name of the convention	Content of the convention
In July 2000	《 Okinawa Charter for the Global Information Society》	The leaders of the United States, Japan, Germany, The United Kingdom, France, Italy, Canada and Russia on Wednesday issued the Okinawa Charter of the Global Information Society, which aims to promote the development of information and communication technologies, narrow the development gap between countries and regions, and build a global information society.
In September 2011	《International Code of Conduct for Information Security》	The document puts forward a series of basic principles on the maintenance of information and cyber security, covering political, military, economic, social, cultural and technological aspects. Stresses the responsibility and right of States to protect national information and cyberspace and critical information and cyber infrastructure from threats, interference and attacks; Establishing a multilateral, transparent and democratic international governance mechanism for the Internet; Fully respect the rights and freedoms of information and cyberspace in accordance with the laws of all countries; To help developing countries develop information and network technologies; Cooperation in fighting cyber crimes.

Since the last century, various international organizations and regional alliances, including the United Nations, have tried to establish an international data and information security system to varying degrees. However, due to the lack of coercive power or interference from power politics, most of them have achieved little effect. However, there is no unified international convention for the protection of network information in various

countries.[10,11]Different countries have different protection policies for data and information rules, and their interest demands are also different. These differences directly hinder the introduction of the international standard national data and information security maintenance convention, which makes it more difficult for multinational enterprises to protect their rights, and also gives some countries the opportunity to "exploit loopholes".

4. CONCLUSION

As incidents involving the data information security conflict between different countries become more and more, the data in different countries of the importance of information security is also rising, then the data in the field of information security related to the establishment of the international convention should also on the agenda, clear related rights and obligations of each sovereign state to ensure that the "TikTok" in this type of event occurs, the body of the violations to channels, to safeguard the legitimate rights and interests of oneself.

REFERENCES

[1] Z.S. Deng, J.M. Dai. International Conflicts restricting cross-border data transmission and Enterprise Response. Research on Network Information Law, 2018(01):182-203+313.

[2] X.R. Gu. Research on international Legislation of Network Security. Gansu University of Political Science and Law,2018.

[3] S.W. Wang. The General Trend of China in the Internet Era -- Multi-dimensional Observation of "Internet +". People's Forum · Academic Frontier, 2015(10):15-24.

[4] X.B. Zhang. On international Rule-making of Network Information Security Cooperation. Zhongzhou Journal, 2013(10):51-58.

[5] P. Yu, Z.Y. Xie. A review of American information security legal system and its reference significance for China's information security legislation. Law School, China University of Political Science and Law. School of Law, Shandong University of Economics.2009.

[6] Y.P. Jiang, Y.J. Li, H.W. Wang. National Network Information Security Strategy. School of Management, Harbin Institute of Technology.

[7] T. Hua. Network Information Security and the Establishment of international information security system in the era of globalization. Nanjing University.

[8] X.B. Zhang, On international Rule-making of Network Information Security Cooperation. Legal Research.2013.

[9] W.M. Wei, Y.Y. Yang, Y.Q. Zhang. A Brief Analysis of good Audit Cases of Information Security Management System. School of Computer Science and Technology, Shanghai Dianli University. 2009.

[10] Z.X. Huang. United Nations Information Security Working Group in the first half of 2020. China. Information Security Cyberspace Strategy Forum.2020

[11] B.X. Fang, P. Zou, S.B. Zhu. Research on Cyberspace Sovereignty. China Cyberspace Security Association. 2016.