Management and Science, Vol.4 No.1 2024, pp. 37-45
ISSN :3078-4123

Construction of security obligation standards for network platforms in cross-border digital flow

Li-xue Wang*

school of law, Qingdao University of Science and Technology, Qingdao, China

*Corresponding author

Abstract: The rapid development of network technology has also brought new digital risks. Along with the large-scale cross-border digital flow, new requirements are also put forward for the network platform to maintain network services. Cyberspace is a virtual public place. As the provider of network services and the manager of cyberspace, the network platform should assume certain security obligations to the users who accept its network services and the country to realize the network digital information security of users and the country. This paper analyzes and discusses what kind of security obligations, the content of obligations and the standards of obligations that the network platform should undertake, in order to promote the scientific construction of the security obligations of the network platform in cross-border digital flow and promote the improvement of digital security in China.

Key Words: Network platform; security obligation; cross-border digital flow

1. Introduction

In the Internet era, digital has become an important data to realize the operation and development of human economy and society. With the cross-border exchanges of countries around the world, the scale of cross-border digital flow is becoming larger, and the cross-border flow of digital has become a normal. The larger the scale of digital cross-border flow, the more information contained in the digital, and various phenomena are complicated and disorderly. In order to protect China's digital security, we must strengthen the supervision of China's cross-border data.

In today's world, the cross-border digital flow is not free, but this freedom is not because the technical level cannot support the cross-border digital flow, but because of the inconsistent attitudes of countries on the cross-border flow of numbers, leading to the current standards for cross-border digital flow. There are many reasons for the obstruction of cross-border data flow. Countries pursue the realization of digital security and safeguard their own digital sovereignty, and expect the realization of digital flow to bring corresponding economic value to them, resulting in the conflict of value orientation. When it comes to the security and efficiency of data cross-border flows, we do not need to choose one of them, but more importantly, we need to consider what benefits are at a higher value level. In the long run, the efficiency value of digital security and digital flow should put the value of digital security first, so how to achieve the security of digital cross-border flow requires the joint efforts of multiple subjects.

The network platform is a network space operated by civil private subjects and providing Internet technical services to the unspecified public. From this perspective, the network platform has its subjective characteristics, and can be understood as the operating enterprise of the Internet platform. With the development of digital technology, the network platform, as the carrier of data, has a huge data information, which can use the information created by the platform or collected by users from the platform. As a master of data, the network platform has enough capacity to supervise digital data and help the security of digital cross-border flow, which is also the most efficient approach. At the same time, as a public organization to a certain extent, the network platform should not only gain huge benefits through the data it has, but also assume higher obligations, starting from the source to become the first line of defense to protect China's digital security, and realize the unity of rights and obligations.

At present, China's network platforms are more liable for tort. When the network users suffer damage, they fail to fulfill the obligations. However, such regulations obviously have defects. The premise of the network platform is that the rights of the users of the network platform are

infringed and notified to the network platform. As a result, the network platform needs to assume a "post-stop-loss obligation", but not a "pre-guarantee obligation". The infringement has occurred, to stop the loss, in fact, to reduce the positive obligation to the network platform, is a way of putting the cart before the horse.

Security obligations stipulated in our country "civil code" article 1198 stipulates the place managers should be into the management of the physical space of the personal and property security security obligations, and look to the virtual network space, we did not introduce the concept of security obligations to virtual space managers within the scope of obligation standards. With the reality

2. The theoretical basis for the cross-border network platform to undertake security obligations

At present, it has become a consensus to realize the strict obligation standards of network platforms. For example, Article 58 of China's Personal Information Protection Law stipulates the four obligations of large network platforms as the gatekeeper of personal information protection. These four obligations not only include the obligation that the network platform should undertake to handle the data and information, but also include the obligation of the network platform to supervise and manage the digital data activities of the provided products or services built within the network space.

Including in the judicial practice, it also puts forward higher requirements for the obligation standards of the network platform. In the case of copyright infringement by 15 people, including Liang Yongping and Wang Zhenghang, in the case No.193 issued by the Supreme People's Procuratorate in 2023, it is obvious that judicial organs have put forward a higher standard for the duty of care of online platforms. The scope of the word "know" in the judgment criteria of safe haven rules in network platforms is raised from "knowing" to "should know".

In this context, it is not abrupt for network platforms to assume more stringent responsibilities. In today's world, digital data carries out large-scale cross-border flow, and this situation puts forward higher requirements for network platforms, and the obligation standards proposed by network platforms are not commensurate with the huge benefits they gain. Online platforms should meet higher obligation standards to meet the requirements of the current large-scale cross-border data flow form. Therefore, we propose, can the network platform assume certain "security obligations" for some subjects participating in network activities? We can learn from the relevant principles of Germany's mature theory of security guarantee obligation, "Those who open or join the communication space have the security obligation to others, and should take care of the rights and interests of others within reasonable limits". Based on this, we can start the discussion on whether the network platform that opens up the network interaction space needs to assume the security obligation of the subjects who join the cyberspace and enjoy the network services.

Security obligations apply to cyberspace

Different types of network platforms provide different types of network services, and the virtual network space formed by the aggregation of target groups gathered by different types of network services is also different. Even though the virtual cyberspace is diverse, they still contain similar characteristics, such as the interaction of the cyberspace, the relative openness, and the unspecificity of the participants. At this point, even if the cyberspace does not have such a fixed place as the real physical space, these characteristics contained in the cyberspace are similar to the reasons why the public place manager of the physical space needs to assume the security obligation to the physical public place.

The manager of public places should assume the security guarantee obligation for the public places under their management because this place is public, management and service. Obviously, these characteristics also have characteristics in cyberspace. Network platform allows not specific social public registration, become the user in the network space built up after the interactive network behavior, these behavior to at least observe the user agreement of the network platform, at the same time by the management of the network platform, and network platform

building network space is in order to provide network services.

Since the cyberspace built by the network platform is used to provide public services and can manage this space, even if the cyberspace does not have an entity, the network platform should also assume the security obligation for it.

The main basis for the network platform to undertake security obligations

As the controller of the network virtual space, the network platform relies on its powerful Internet technology and has a strong openness and inclusiveness. The network platform has expanded a huge root system and formed a huge business empire. Due to the prominent importance of its own technological development and the theory of platform supervision responsibility, the pre-management obligation of the network platform should also be valued. The network platform shall be the undertaker of the security guarantee obligation within the corresponding control scope.

1. Definition of the network platform

Why do we let the network platform assume the subject of the security obligation of cyberspace? What kind of existence is the network platform? Clarifying this problem is a prerequisite for the network platform can be regarded as the subject of security obligations.

First of all, it can be clear that the network platform as a subject, the existence of the platform must be real, and should be built by the real natural person or legal person as the owner of the platform. The purpose of this platform is to provide a certain kind of network service, thus attracting users to aggregate in a virtual network space, making this space become a medium to realize the purpose of its network service. Providing network services, of course, also requires the platform to have certain technology and equipment, and the platform can actually control the cyberspace through its master technology and equipment.

From this, we can define the network platform: the network platform is the controller and owner of the network space built by the network technology and the network equipment and the network services provided by it. In this paper, the network platform is similar to the existence of the network service provider, that is, the natural person, legal person or unincorporated organization that provides the network service for the purpose of the network service and the establishment of the service medium.

2. The dominant position of network platforms in undertaking security guarantee obligations

The dominant position of the network platform to assume the security obligation is firstly based on the perspective of legal economics, and who is assigned to the obligation depends on who pays the lowest cost to undertake this obligation. Whoever should assume more obligations for the good operation of cyberspace and the smooth flow of digital data is bound to build this network platform in cyberspace. At the beginning of the establishment of the network platform, the purpose and mode of digital generation and flow in the network space have been determined. The network platform has an absolutely powerful Internet technology in the network space that it controls, and can clearly grasp whether there is any abnormal situation in the data flow through its powerful technical means. At the same time, because of the absolute dominance of the network platform over the network space, once the data is abnormal, effective measures can be taken to eliminate the risk of abnormal data flow in the network space with the minimum cost.

From the perspective of danger control theory, if a person creates or maintains a risk that may cause damage to others, and taking a measure to avoid it is not beyond his ability, then it becomes an obligation to take such a measure. It can be proved that the generator of danger has enough opportunity to reduce the risk within their capacity. Network platforms provide network services to generate data flow in cyberspace, which may cause data leakage, data abuse, and national data sovereignty damage and other dangers, and damage the network level.

The target of cross-border network platforms for security guarantee obligations

In the context of cross-border digital flow, the objects of security obligations of

network platforms should include not only natural persons, but also the country.

The object of the public place security right holder assuming the security guarantee obligation is the unspecified subject that enters the public place under its management. Non-specific objects who enter the cyberspace and accept the services provided by the network platform are the network users who register on the network platform. These network users store all or master the information in the network platform, and allow the network platform to use their information to generate new data. Then, the network platform should assume the security obligation to these non-specific network users.

The digital information mastered by the network platform is not only the economic means of production, but also the important national strategic data. The state is also the object of network platform activities and accept network services. Digital data containing national information is also stored in the storage media of the network platform. The cross-border network services provided by the network platforms deeply affect the national digital security. The data stored in the network platform containing national biology, electronics, economy, science and technology information may lead to the leakage of state secrets once the cross-border flow flows. If data from other countries 'hegemonism, power politics and terrorism flow into China's cyberspace, it may endanger national sovereignty and security. Therefore, the state should also become the obligation object of the network platform to undertake the security guarantee obligation.

Based on the characteristics of the civil legal subject, the state is the object of the network platform to undertake the security guarantee obligation, and the state and the network platform are equal civil legal subjects. However, when the state is used as a user of the network platform, the information stored on the network platform will contain more social and public interests and national security interests. Because of the particularity of the national subject, the security obligation of the network platform to the country may surpass the original concept of security obligation in the civil law, and have the color of administrative law.

3. Cross-border network platforms to undertake security obligations

It fying the subject and object of the obligations, and the content of the security obligations should be clarified so as to clarify the scientific construction of the security obligations of the cross-border network platform. In view of the existing needs of cross-border digital flow, building network platform security obligations is a good way to build scientific obligation standards. The standard of the guarantee obligation is constructed, and the corresponding responsibility standard should be constructed to guarantee the realization of the obligation. In this way, the basic content of the security obligations undertaken by the cross-border network platforms is basically determined.

Data flow requirements for platform security obligations

At present, the relevant legal regulation system of cross-border digital flow in China should be established on the basis of the dynamic balance of "freedom-regulation". Therefore, the security obligations of China's cross-border network platform should be formulated to safeguard national security while taking into account the needs of cross-border data flow. The efficiency and security of cross-border data flows need to be effectively combined.

It should also be noted that the security obligations of network platforms should not be excessive. One of the preconditions for network platforms to assume the security obligations is that they gain huge benefits by providing network services, so they should assume the matching obligations for their profits. Therefore, the security obligation undertaken by the network platform should not exceed the scope of its profit, and the security obligation undertaken by the network platform should not affect the continuous provision of network services and healthy and stable development of the network platform. In the context of cross-border data flow, network platforms assume too high security obligations, but may not be too good. It

can lead to significant operating pressure for platforms; significantly less purpose for users in using the network; and a barrier to the development of digital technology itself.

Network platform security guarantee obligation content framework

At the level of the network platform security obligation can be divided into two parts, namely, the protection of the network platform, namely the data carrier, and the protection of the network data and information.

Combined with the relevant provisions of the Network Security Law, network security can be divided into four fields: network service security, network operation security, network data security and network information security. Network service security requires that network platforms must uphold good faith when providing network services, not maliciously set up procedures with obvious loopholes, and timely disclose the security risks in technology or equipment when network platforms are providing network services. Network operation security refers to that the network platform should provide different levels of security protection measures for the network space of different service targets to prevent the attack and invasion of viruses and Trojan horses. Network data security requires network platforms to protect the collected and derived data, prevent data loss or malicious theft through classification, encryption and backup, strengthen the protection of network users' personal information and state secret information, and prevent such information from illegal acquisition or illegal flow of such information. Network information security refers to the network platform must first to strictly implement the real-name system, security network data and information can be traced, found illegal, illegal information or may violate the rights of others, actively take the corresponding technical disconnection, delete, shielding to prevent the expansion of the infringement. It can be seen that network service security and network operation security are both regulated by the network platform on the carrier of network data and information, while network data security and network information security are to protect the essence of network data and information. Therefore, the network platform should take into account the domestic data information security and cross-border data information security in assuming the security guarantee obligation, and promote the network platform security in terms of network service and operation.

In terms of the specific content of the security obligation of the network platform, the network platform should realize the minimum security requirements for fulfilling the security obligation. At least the following should be done:

Service sustainability obligation: The purpose of the network platform is to realize its network services, realize certain data interaction, and create economic benefits of Internet services. The sustainability of service means that when the network service collapses or interrupted due to technical and equipment reasons, and the purpose of network service cannot be temporarily realized, timely measures should be taken to repair the existing problems, restore the network connection, and ensure the realization of the purpose of user interaction on the network platform.

Virus, Trojan prevention and vulnerability remedy obligations: virus, Trojan is the most common computer attack program, network platform to realize the normal operation of the platform, will take measures to check whether there is a malicious program trying to attack its network server, at the same time to detect the existence of malicious plug-ins and attached to the spread of network services. Once the virus or Trojan horse is successfully invaded, then the server controlled by the network platform will inevitably leave certain loopholes. At this time, the network platform should assume the obligation of actively responding to it and actively remedy it. In the process of cross-border data flow, network platform to deal with malicious program is likely from overseas, organized malicious attack, once its successful invasion of our network platform, our country's network security must suffer huge losses, so the network

platform in the face of foreign malicious program attack, have to carefully deal with.

Data information review, supervision obligation: data information review, supervision obligation is the network platform to accept, and as a media data information content to a reasonable review obligation, it should be seen as a network platform as data information interaction platform attached obligations, is also a kind of positive means to prevent illegal, illegal information diffusion. In the process of reviewing the data information, the network platform needs to bear the obligation of "notification-delete" to the general infringing data information. When the infringed notifies the network platform that its rights are infringed, the network platform should take necessary measures in time to prevent the further expansion of the damage. But for our country "Internet information service management method" nine clearly mentioned in article 15 of the Internet platform shall not production, copy, release, dissemination of Internet data information shall undertake strict censorship obligations, to the utmost possible and efforts, monitoring such data information exists, and found timely shielding, delete relevant content, and keep records, and fulfill the obligation to timely report to the state organs. However, the "nine prohibitions" stipulated in the Administrative Measures of Internet Information Services in China is of great significance in today's large-scale cross-border flow of data and information. The existence of these nine types of digital information, whether flowing from abroad or flowing from China, may infringe on the stability and unity of China.

Data security management and security obligations: Data security requires that the data is complete and reasonably protected. The standard of reasonable protection obligation is that at least the data can not be accessed and known by unauthorized users, and shall not be tampered with or damaged by network users as the subject of private law. The security management and guarantee of data and information should be regarded as the core of the security
guarantee obligation of the network platform. As the basis of cyberspace security, data security itself is closely related to national security and economic development, personal privacy protection and social stability. Once data is leaked and abused, it will face huge network risks. In today's tense international situation, cyber risks will become a severe challenge.

Assist law enforcement and judicial obligations: any subject should become the defender of public interest and national security, which is the obligation of every citizen, and also the social responsibility that every citizen should bear. As the gatekeeper of national network security, the network platform should of course assume the obligation of assisting law enforcement and justice. As the medium of network activities, the network platform can rely on the advantages of its cyberspace controller to help realize the law enforcement and evidence collection of digital crime and digital infringement, and provide help and support for the acquisition and fixation of evidence. While assuming the obligation of assisting law enforcement and justice, network platforms should also pay attention to assuming the corresponding confidentiality obligations in the process of law enforcement and justice.

Cross-border network platforms violate the standards of security guarantee obligations

As a network platform, the volume of data and information it accepts and stores is very huge. Even if the network platform tries its best to fulfill its security obligations, it cannot completely eliminate the abnormal flow of network data and information, and it is difficult to completely resist the network attacks of willing people. In order to realize the absolute security of network data, it is not enough to rely only on the network platform to undertake the security obligation, but the network platform is still the most effective way to protect the network security under the background of cross-border digital flow. Therefore, we do not have to demand the network platform to assume excessive security obligations, only need to make the

network platform to assume moderate security obligations.

What kind of obligation standard can be identified as the network platform to assume sufficient security obligations, which should be considered in combination with the case situation. However, we can still not completely generalize certain general standards to measure whether the network platform has fully assumed its security obligations.

First of all, the network platform should start from the rationality standard when assuming the security guarantee obligation. As a platform to master technology and knowledge, the network platform has professional knowledge structure and technical ability, and should fulfill the cautious and rational obligations that a professional subject can fulfill. From the flow of network data, the network platform itself provides a certain risk of digital data leakage when providing digital network services. The degree of security obligations of a network platform should at least be balanced with the risks it creates while providing services. As the creator of danger and the manager of cyberspace, the security obligation of the network platform should be higher than the obligation of ordinary network users to protect their network data and information. The reason for making such a judgment is that the network platform has a better understanding of the risks generated by data flow in cyberspace, has a higher ability to foresee the risks of data flow in cyberspace, and is more likely to take control measures to reduce the risks.

The standard degree of network platforms to undertake security obligations should also refer to the principle of fairness. Considering the theory that the benefit and the risk are consistent, the cost of the security obligation assumed by the network platform and the benefits obtained by the network service provided by the network platform should form a relatively reasonable proportion range. Under the background of the large-scale cross-border flow of network data, the income of the network platform has been increased greatly compared with the income of the network data
only flowing in China in the past. Then, cross-border network platforms should assume higher security obligations than in the past. The proportion of the expenditure incurred by cross-border network platforms and the income from providing network services should also increase with the expansion of the scale of cross-border data flow. This is because in the cross-border data flow, the security obligation undertaken by the network platform contains the protection of national data security, which is higher than the protection of personal interests, national security is above all else, and the network platform for national security is slightly higher than the past obligation standards and reasonable and worthwhile.

Network technology is constantly developing and progressing, and the standard of network platform to undertake security obligations should also be along with the progress of network technology. When judging the security obligations of the network platform, we should start from the comprehensive standards and treat them scientifically. Case analysis is conducted based on the situation of each specific case. From the perspective of users' trust interests, in order to protect the trust interests of network users, it is not enough to only let the network platform assume the security obligation, but the security obligation of the network platform is the first to bear the brunt. If the network platform is required to assume the security obligation by law, then this obligation is at least compatible with the technical level of the network platform. To meet the reasonable expectations of network users, network users expect the network platform to create a safe and healthy network environment. The part of network users beyond reasonable expectations does not belong to the part that the network platform should assume security obligations. The expectation that the network platform will undertake the protection obligation of national data security is a reasonable expectation with high value, and the guarantee obligation for the security with higher value level also puts forward a higher

security guarantee obligation requirement for the network platform.

Allocation of responsibility for cross-border network platforms for violating security obligations

Network platform must be implemented as a security obligations, when the network platform in practice, should bear the corresponding responsibility, if choose to not as behavior, but also chose the network data flow order collapse and network users of law, network platform, will also lead to national data sovereignty. Therefore, when constructing the security obligation of the network platform, we should also build the standard for assuming the responsibility of the network platform for violating the security obligation. Through the establishment of the corresponding responsibility system to force the network platform to better undertake its due security obligations.

Before the responsibility distribution, the responsibility principle of the network platform should be clarified. This paper holds that the network platform can adopt different imputation principles when different objects bear the tort liability caused by the failure or incomplete security guarantee obligations.

To judge whether the network platform has fulfilled its security obligation to ordinary network users, it should follow the presumption of fault responsibility. If the network platform assumes the no-fault responsibility to the network users or the country, it may seriously reduce the enthusiasm of the network platform to provide network services, and the guarantee obligation to the network platform is too high, which will hinder the continuous development of the network platform. However, in the network space, the network platform and the network users are not in an equal position. Compared with the network users, the network platform is obviously in a strong position. Network users want to prove that the network platform has the fault and make the network platform bear the fault responsibility, so the difficulty of proof is very high. Due to the burden of proof of the presumption of fault, the burden of proof of network users can be reduced. Through the principle of presumption of fault, the network platform is required to prove its innocence and require the network platform to fulfill its security obligations. There is no subjective fault, which effectively urges the network platform to better fulfill its obligations in the process of providing services.

When the network platform does not assume the obligation of security protection, its omission will lead to the infringement of the network users' data security rights and interests, and the network platform is intentional or negligent in its omission, the network platform shall bear the tort liability for the damage of the rights of the network users. When the right of network data is infringed, if no third party intervenes, the network platform shall bear all the tort liability. In the case of the intervention of a third party, whether the network platform should also bear the tort liability should judge the size of the force of the third party in the tort consequence based on the intervention of the third party, and then distribute the liability.

When the state is the object of the security obligation of the network platform in the cross-border data flow, the network platform shall bear the no-fault responsibility of the state. When abnormal data cross-border flows are generated, there will be countless opportunities for online platforms to take measures to ensure national data security. When national data security is effectively violated by cross-border data flow, it is bound to have experienced cross-border digital attacks for a long time. Under such circumstances, no matter whether the network platform properly undertakes the security obligation, it is difficult to isolate it from the final infringement result. And because of the national data security which contains the high public interest, national digital security once violated, the loss is difficult to measure, these reasons require network platform for national digital security higher security obligations, network platform for the state of inappropriate security obligations of tort liability should also be applied when more stringent liability.

4. Conclusion

General Secretary Xi Jinping has stressed for many times that data has become a new factor of production, which has had a huge impact on the traditional mode of production and driven the reform of the traditional mode of production. Therefore, ensuring national data security is the requirement of the current situation of social production and life.

The cross-border flow of data is the trend of The Times. With today's rapid development of science and technology, we need to deal with the challenges brought by the digital cross-border flow. Under the background of the digital cross-border flow, the network platform should first continue to do a good job in guaranteeing the digital information of the network users entered by its platform. At the same time, it is also necessary to respond to the risks of national digital security in the cross-border digital flow. In the context of cross-border digital flow, online platforms should be considered what obligations should be raised and to what height should be raised.

With the development of cross-border digital technology, the management ability of the network platform relying on its technology and equipment is constantly improving. In the network space, the management position of the digital information created or absorbed is increasingly prominent. In order to maintain the sustainable, stable and healthy development of cyberspace for a long time, online platforms need to assume more responsibilities.

A network platform should assume security obligations to the network users and the state, and this obligation should be regarded as a collection of a class of obligations. This collection should include a set of separate obligations that can help with data management and facilitate the security of data flows across borders.

Asking the network platforms to assume the security guarantee obligation for the network users they serve is an effective move to ensure the stable flow of data and enhance the technical information of the network users to the domestic digital service platforms. It is also a necessary measure to urge
the network platforms to undertake the corresponding social obligations and realize the unification of the rights and obligations of the network platforms. First of all, the digital security of ordinary network users can better guarantee the digital security of the country. In the cross-border flow of network digital, the country should also be regarded as the object of the security obligation of the network platform. When the state is the obligation object of the security guarantee obligation of the network platform, of course, it puts forward higher requirements for the security obligation guarantee standard undertaken by the network platform.

Making the network platform assume scientific and reasonable security obligations cannot fully cope with the technical risks brought by the rapid development of digital technology in the current era and in the future. The rapid development of network technology will put forward different requirements for the network platform. The research on the obligation of network platform should be combined with the guidance of multi-perspective legal theory to promote the improvement of the obligation of network platform and promote the guarantee of China's digital network security.

Reference

[1] Wang Jingwen, Yang Dengfeng. Give a specific network platform the status of an organization authorized by laws and regulations [J]. Social Science in Xinjiang, 2024, (02): 104-113.

[2] Wang Siyuan. On the security obligations of network operators [J]. Contemporary Law, 2017,31 (01): 27-37.

[3] Cheng Xiao. Civil liability of large network platforms for violation of gatekeeper obligations [J]. Legal Science (Journal of Northwest University of Political Science and Law), 2023,41 (05): 32-41.

[4] Wang Jie. New solution of the duty of care of the network storage space service provider [J]. Legal Science (Journal of Northwest University of Political Science and Law), 2020,38 (3): 100-113.

[5] Liu Wenjie. Security assurance obligations of network service providers [J]. Chinese and Foreign Law, 2012,24 (02): 395-410.

[6] Li Yuanju: Network Security and Criminal Responsibility of Platform Service Providers, Law Forum

[7] Li Hao. Theory on Transaction Security Duty- -An Interpretation of the Structural Changes of German Tort Law [M], Peking University Press, 2008.

[8] Jiang Chengxu. The principle of trust interest protection from the perspective of survival theory [J]. Oriental Law, 2016, (04): 71-79.

[9] Huo Yongku, Feng chic. Analysis of social role theory [J]. Journal of Xi'an Jiaotong University (Social Science Edition), 2016,36 (01): 62-68.

[10] Wen Ming, Li Xingyi. Cross-border data flow governance and China Scheme under the framework of "Freedom-Regulation" [J]. China Science and Technology Forum, 2024, (04): 106-116.

[11] Luo Zhimin, Chen Jinyi. On the hybrid regulation of the network platform [J]. Journal of Dalian University of Technology (Social Science Edition), 2024,45 (03): 71-79.

[12] Wang Hongcheng, Cao Liping, Li Dongtao. On the focus of infringement cases of video sharing websites [J]. Electronic Intellectual Property Rights, 2009, (04): 11-16.

[13] Zheng Sen. Research on higher Duty of Care for Network Service Providers in the Age of Intelligence [J]. Henan Science and Technology, 2024,51 (08): 123-126.

[14] Guo Xuejiao, Gao Tianshu. Cross-border data flow: realistic dilemma and cracking path [J]. Southern Finance, 1-11.

[15] Chen Aifei. "Data Controller standard" forensics mode and China response [J]. Legal Research, 2024,41 (03): 60-74.

[16] Guo Dexiang. Multiple dilemmas and path innovation of data exit security governance in China [J]. Legal Commentary, 2024,42 (03): 170-181.

[17] Xing Huiqiang, Li Zehui. China's cross-border personal data flow certification system and its improvement [J]. Journal of Zhengzhou University (Philosophy and Social Sciences edition), 2023,56 (06): 54-60.

[18] Tan Guanfu. China's regulation on digital trade under the perspective of international economic and trade rules [J]. Hebei Law, 2023,41 (12): 134-157.