Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 6, No. 2, 2024

The Rule Boundary of Network Platform Security Guarantee Obligation

Yiting He *

School of graduate, People's Public Security University of China, Beijing, China
*** Corresponding author Email:** 384856174@qq.com

Abstract: Network platform, as the engine of economic development in the new era, is filled with all aspects of communication, information exchange and resource circulation in modern life. Disputes cannot be avoided in the process of participating in social life. While the network platform is active, it also produces many judicial practice problems with the characteristics of the network era, such as the network platform infringement. The problem of infringement in the Internet era has the characteristics of virtual abstraction in cyberspace. Different from traditional dangers such as kidnapping and intentional injury, Internet users may also face new risks such as cyber violence and loss of virtual property. The theoretical legitimacy of applying the security guarantee obligation from physical space to cyber space can be discussed from the aspects of subject nature, legal basis and legal variability. The content provisions on the security obligations of network platforms in the Civil Code are still vague, and the specific scope of application of the rules is limited. This paper tries to determine a reasonable content boundary from the perspectives of platform service types, benefit-risk principles and cost-benefit principles. Based on this, it further analyzes and defines the types of responsibility that the network platform should undertake under different circumstances in violation of security obligations.

Keywords: Network Platform; Security Obligations; Regulatory Boundary.

1. Introduction

With the continuous penetration of network technology into all aspects of people's lives, daily clothing, food, housing and transportation are inseparable from the participation of network platforms, and network security accidents occur frequently. As one of the important subjects of Internet infringement disputes, the identification and division of responsibility of network infringement cases have attracted wide attention and discussion. [1] Although a relatively perfect system framework has been established about the obligation of security assurance in our country, with the development of science and technology, a new application situation has emerged for the obligation of security assurance. The legislation should consider whether the obligation of security assurance should not be limited to the traditional physical space domain, and cyber virtual space is also taken into account to assume the scope of the obligation of security assurance. The relevant legal provisions of China's network platform security obligation are fragmentary, and there are problems of blurred boundary rules, which leads to the difficulty in identifying the network platform security obligation and liability in the judicial practice of network infringement cases, and it is difficult to protect the legitimate rights and interests of network platforms and network users.

2. Basic Overview

2.1. Definition of Network Platform

"Network platform" can also be called "Internet platform", is the product of the Internet era under the rapid development of science and technology. The "platform" here is similar to the concept of "platform" in economics. It is a service medium to assist information communication and resource exchange on the network, such as shopping platform, travel platform and social platform. China's laws and regulations do not give a clear definition of "network platform". "Network service provider" and "network platform" often appear in some network infringement cases, but the conceptual difference between the two is not clear. In fact, there is little difference between the two terms in essence, and the difference between the two can be analyzed from the nature. [2]Network platform only refers to the network service provider who acts as a service intermediary, and can be identified as a special type of network service provider.

2.2. The Legitimacy of Network Platform Security Guarantee Obligation

The traditional subject of security guarantee obligation is the manager or organizer of offline physical space. However, with the continuous development of science and technology, online virtual space subjects such as network platforms have appeared in social life. Whether the law should include virtual space into the subject scope of security guarantee obligation has become a hot dispute in the field of legal theory.

From the point of view of subject nature, the subject of traditional security obligation refers to the manager and operator of the offline physical space. The trading place of the online platform is different from the traditional offline trading place, which is a virtual trading place supported by technology and data. Both are essentially trading platforms for merchants and consumers. The online platform is the manager and operator of the online virtual space, whether online or offline, is the manager and operator of the space, and should have the security obligation for the conduct of the transaction.

From the perspective of legal provisions, Article 1198 of the Civil Code stipulates that managers and operators who fail to fulfill their security obligations should bear the corresponding civil compensation liability. Article 38 of the E-commerce Law also stipulates that network service providers who fail to fulfill their security obligations should bear the corresponding liability for compensation. Network platform belongs to a special category of network service

providers, and it is also the manager and operator of online virtual transaction space, so the above security obligation provisions should also be applied, and there is a legal basis to support its existence.

3. The Applicable Restriction of the Security Obligation

According to the above analysis, this paper believes that there is a certain theoretical basis for network platforms to undertake the security guarantee obligation, but the security guarantee obligation is also a kind of responsibility burden in essence, if not controlled, it will become an unfair network platform.[3]This paper tries to limit the application of security obligation to network platform from three aspects: platform service type, benefit-risk principle and cost-benefit principle.

3.1. Network Platform Service Type

With the continuous upgrading of modern Internet technology, the network platform has gradually developed and increased life services such as payment and borrowing, consumption and shopping, travel and taxi hailing, takeout food, learning and communication from a simple information exchange medium. The different content and nature of the service types of network platforms determine the different emphasis of security guarantee obligations undertaken by each type of network platforms. [4]For example, social chat software needs to protect the privacy and security of users, travel taxi software needs to verify the driving qualifications of drivers who receive orders, and search engine software needs to ensure the real legitimacy of information. Different platform types and service contents lead to differences in technical support, platform design and functional purposes of network platforms, and the specific content of security obligations of network platforms should be determined according to different service types.

3.2. Income-risk Principle

Benefits and risks are in direct proportion, and economic entities should also assume corresponding responsibilities and obligations when they obtain high returns, so the size of the security obligation of the network platform is proportional to the size and correlation degree of the benefits obtained from its business activities. While providing service functions, network platforms will charge service fees, and even if they do not charge service fees, they will obtain profits from other aspects. Therefore, it is reasonable for network platforms to undertake certain security obligations. The obligation of network platform to provide security protection protects the legitimate rights and interests of network users, which is in line with the interests of society and the interests of the long-term sustainable development of network platform. The security guarantee measures of the network platform maintain the trust interests of the network users, and help the platform accumulate long-term user resources, which are the lifeline of the survival and development of the platform. The greater the profit of the network platform from the network transaction, the higher the degree of profit correlation, the greater the responsibility should be borne.[5] For example, direct profit methods, such as drawing dividends or collecting rent, should carry a higher security obligation than indirect profit methods, such as obtaining advertiser investment through trading influence.

3.3. Cost-benefit Principle

The cost of the network platform to fulfill the security obligation and whether it has the ability to predict and avoid the occurrence of infringement should also be taken into account in the undertaking of the platform's security obligation. The network platform is an online virtual space, which means that it has a certain openness and complexity. The scope of supervision required for the platform to find infringement is very extensive, which greatly increases the difficulty and cost of supervision for the platform to supervise infringement. Over-reliance on the network platform to ensure the security of network transactions cannot guarantee the conduct of platform transactions, and is not conducive to the long-term sustainable development of network platforms. Legislation should appropriately limit the regulatory obligations of network platforms to ensure the maximum protection of network users at a reasonable cost.

4. Content of Network Platform Security Guarantee Obligation

Clarifying the content boundary of the security obligation applied to network platforms is conducive to standardizing the application of security obligation, and provides a thinking path for the court to identify the responsibility in practical trials. The following will be defined from three different stages before, during and after the network platform undertakes the security guarantee obligation.

4.1. Pre-safety Obligation – Prevention

The obligation of security guarantee in advance refers to the obligation of the network platform to actively prevent risks and eliminate security loopholes in network communication in advance in order to protect network users from infringement. The limit of risk prevention obligations undertaken by the network platform in advance should also be determined according to the characteristics of the platform service, the platform's foresight ability and the possibility of preventing infringement acts. The limitation of specific conditions should not be ignored and the burden of platform risk prevention should be increased blindly.[6] In practice, the obligation of risk prevention in advance is mainly manifested as the active measures taken by network platforms to reduce the possibility of risk occurrence, such as reviewing the qualification of platform operators, warning risks and maintaining network operations. The qualification audit obligation is that the platform verifies the qualification identity of both platform operators and platform users, and distinguishes and restricts the high-risk groups of infringement. This obligation is more like a threshold obligation, which minimizes the possibility of violation of laws and regulations of platform users. After users enter the platform, they should still maintain the review of their subsequent operations. The obligation of warning risk means that when the platform detects the possibility of risk occurrence, it gives an early warning of risk to the network users in advance. For example, Taobao uses historical consumer review statistics to score a store and remind consumers that the store may have quality or service problems. Maintaining the obligation of network operation is that the network platform provides a secure trading environment for network transactions with the technology it has mastered. For example, encrypt important private data to prevent user privacy data leakage caused by hacking, or improve the

transaction payment process to enhance the security of funds. Cyberspace is a virtual space, there are unknown risks, can not be like the traditional physical space can take specific security measures in advance, such as arranging security personnel in public places, supermarket commodity sampling, etc., can only be based on the nature of the platform service and technical capabilities, develop the platform's own characteristics in advance security measures. In practice, it is often difficult to entrusts the platform with mandatory prior security obligations according to the law, and enhancing the voluntary performance of the platform's security obligations can better protect the transaction security of network users.

4.2. The Duty of Safety Guarantee in the Event – elimination

The obligation of security guarantee in the event refers to the obligation of the network platform to stop the network accident in time, cut off the source to avoid the expansion of losses and investigate potential risks. Risk elimination countermeasures can not only avoid the expansion of losses but also help network users to recover losses in a timely manner, which is no less important than prevention and remediation in advance, which can be mainly divided into two situations, one is the occurrence of infringement, and the occurrence of infringement has been monitored. At this time, the network platform should act in a timely manner to stop and avoid causing losses or expanding losses to network users. [7] For example, the Didi platform for abnormal orders in the journey, timely Internet alarm, to prevent passengers from suffering danger during the journey. This approach in the event of timely risk control, to avoid the platform driver infringement accidents, so as to ensure the safety of platform users. In the other case, the specific risk of infringement is not clear, but it is known that there is a possibility of this risk. At this time, the risk elimination obligation of the network platform is mainly manifested in the supervision and investigation of potential infringement risks. The platform timely reminds the network users who may be infringed, and takes certain measures to protect the users when necessary. For example, online payment platforms freeze funds for a short time for users with high risk of fraud, verify transactions, check risks and then unfreeze them to avoid users suffering huge property losses.

4.3. Ex Post Security Obligation – Remedy

The post-event security obligation refers to the obligation of the network platform to take the initiative to reduce the loss of network users and help them protect their rights after the infringement has occurred. The obligation to remedy the situation after the event is not because the platform is a danger maker, but because the platform is the manager and operating organizer of the public place of cyberspace, and has the obligation to eliminate the potential dangers of the public cyberspace under its management. The specific content of the obligation shall be based on the nature of the platform, the type of service and the type of damage, to develop a reasonable scope of obligations, according to which the platform shall undertake the obligation of help and assistance to network users, and assist network users to protect their rights. Different from the closed transaction of traditional physical space, the online platform has the characteristics of open and complex transactions. Therefore, the post-operation security obligation of the online platform is different from that of the traditional business place to provide direct help. Moreover, the law does not specify the scope of its obligations, and the post-operation assistance obligation of the online platform is more to use its own resources and technical advantages as a platform. Provide relevant information and actively cooperate with investigations and other indirect assistance.[8] It is mentioned in Articles 1195 to 1197 of the Civil Code that after an infringement occurs, Internet service providers shall cut off the links of infringing information in a timely manner or delete relevant infringing content to reduce losses to the infringed. Internet platform is a special category of Internet service providers with intermediary service functions. Internet platforms can also apply the same legal provisions for Internet service providers. Compared with network users and network operators, the network platform has a natural forensics advantage, but it is worth noting that the network platform should not disclose the personal privacy of users and operators at will in the process of assisting in forensics, and should legally assist the infringed to carry out forensics rights protection.

5. Limits of Liability for Breach of Security Obligations

China's law does not have a clear definition of the nature of the liability of the network platform for violating the security obligation, and the Civil Code only puts forward in the tort liability compilation that the subject who fails to fulfill the security obligation "should bear the tort liability". The legal theory circle has been arguing about the nature of the responsibility of the network platform for violating the security obligation. In the process of the designation of the Electronic Commerce Law, the debate on the nature of the e-commerce platform for violating the security obligation has experienced a tangled course of "joint and several - bearing corresponding supplementary liability - corresponding liability".[9] Legislators finally take the expression of corresponding responsibility, which can also represent the attitude tendency of the legal community towards the responsibility of the network platform for violating the security obligation to a certain extent. However, the corresponding responsibility is a general concept, the specific application is not specified in detail, resulting in the problem of different application in judicial practice. This paper tries to further analyze the liability of the network platform for the application of the security guarantee obligation from the causal relationship between the platform and the infringement result, and divides it into three applicable cases: joint and several liability, partial liability or supplementary liability.

5.1. Joint and Several Liability

The network platform applies joint and several liability for violating the security obligation in two situations. Firstly, when there is a subjective and objective competition relationship between the platform and the third party's infringement, meaning that the platform directly assists the third party's infringement and becomes a direct infringer of joint infringement. This type of infringement requires both subjective intentionality from the network platform and its acts being direct causes of infringement. Secondly, when the network platform does not intentionally infringe but fails to fulfill its security obligations, it should bear joint and several liability within the scope of these obligations. The determination of whether joint and several liability is applicable should be detailed and rigorous due to its severity

among three types of liabilities; excessive application would only encroach upon legitimate interests of the network platform, which is detrimental to its long-term healthy development.

5.2. Supplementary Liability

The applicable supplementary liability is limited to the situation where the third party is intentional and the network platform is negligent in assuming the security obligation. The supplementary liability, as the name implies, is complementary to the liability of the responsible body, which is mainly reflected in two aspects. The network platform shall be liable for supplementary compensation for the unpaid part only if it fails to perform or fully perform the obligation to pay compensation. At this time, the third party of the direct infringer is the ultimate responsible person, and the network platform has the right of recourse to it, that is, after paying the infringed party, it can pursue compensation to the third party. On the other hand, the compensation is complementary. [10]The supplementary compensation liability undertaken by the network platform generally does not exceed half of the total amount of compensation, and the specific scope of compensation should be determined according to the specific circumstances of the case.

5.3. Share Liability

Share responsibility means that the network platform only bears the corresponding share of responsibility for its own actions or obligations. The application of liability by share also requires that the network platform's failure to perform the security obligation and the third party's infringement are not enough to independently cause damage. The specific responsibility content is divided according to the fault degree and cause force of the network platform security person and the direct infringer. Different from supplementary liability, there is no setting of compensation sequence, and the compensation obligations of each subject are independent of each other. The burden of share liability is relatively heavier than the burden of supplementary liability, because the failure of the network platform to fulfill the security obligation usually only increases the possibility of the occurrence of damage, not the main reason. Share liability requires the security guarantee obligor to independently bear share liability, which in fact reduces the burden of the infringer and increases the burden of the network platform. Therefore, the legislation should limit the application of the network platform to bear a share of the responsibility for violating the security obligation.

References

[1] Li Yujin. A Preliminary study on the tort liability of network platform operators -- from the perspective of security obligation. Journal of Shanxi Youth Vocational College, 21, 34 (2) : 59-62.

[2] Xu Huiyun. Empirical Analysis and theoretical Approach of e-commerce Platform security obligations: Starting from the second paragraph of Article 38 of the E-commerce Law. Journal of Hubei University of Economics (Humanities and Social Sciences Edition) , 2023, 20(06):80-84.

[3] Mi Xinli; Liu Zhengzhi. On the Security Guarantee Obligation of E-commerce Platform. Administrative Reform,2020.

[4] Li Xiaxu. Legal Basis and system Development of indirect tort liability of network Platform. Research on Comparative Law,2023(03):173-187.

[5] Yuan Xue. Network platform operator safety guarantee obligation research. Jiangsu university, 2023.

[6] LAN Shourong. E-commerce Platform security Obligation from the perspective of Consumer Law. Review of Political Science and Law,2023(02):37-46.

[7] Wang Nijie. On the boundary and structure of the security obligation of Internet Service providers: from the perspective of the interpretation of the network infringement rules of the Civil Code. Rule of Law Research,2022.

[8] Mi Xinli; Liu Zhengzhi. On the Security Guarantee Obligation of E-commerce Platform. Administrative Reform,2020.

[9] Xue Jun. On the Core issues of Network Platform security Obligation in the Civil Code. China Information Security, 2020 (10) : 81-84.

[10] Qi Aimin, Chen Chen. On Transaction security Obligations of network trading platform providers. Journal of Northwest University of Political Science and Law, 2011,29 (5) : 67-74.