# Issues on Sentencing of Network Service Providers in Cybercrime

Huining Hu*

School of International Law, Northwest University of Political Science and Law, Xi 'an, China

* Corresponding Author Email: 202010840440@stu.nwupl.edu.cn

**Abstract.** With the continuous progress of science and technology, the problem of conviction and sentencing of network service providers in the field of cybercrime has become increasingly prominent. In judicial practice, there are often different judgments in the same case, ambiguous sentences in the judgment, and ambiguous qualitative nature of the subject of the crime, which shows that the path of conviction and sentencing of network service providers needs to be improved. Through analyzing the current laws and regulations concerning network service providers in China, the lack of classification of network service providers and the application of relevant sentencing laws are the main obstacles to the conviction and sentencing of network service providers. It is suggested to solve the practical obstacles of conviction and sentencing of network service providers by classifying network service providers, limiting the crime of helping information network crimes, strictly controlling the information network security management obligations of network service providers, and perfecting the relevant legal provisions on the obligations of network service providers.

**Keywords:** Criminal Responsibilities, Network Service Providers, Cybercrime.

## 1. Introduction

With the continuous progress of information technology, the forms of cybercrime are increasingly complex and diverse. China has formulated and revised laws and regulations related to network service providers in accordance with the trend. Article 28 and Article 29 of the Criminal Law Amendment (9) clearly stipulate the crime of refusing to perform the obligation of network security management and the crime of helping information networks, providing a legal basis for the criminal regulation of network service providers. However, both theoretically and practically, there are still obstacles to sentencing ISPs. Some scholars have distinguished the types of network service providers, [1] some scholars have analyzed relevant foreign systems and put forward reference suggestions, [2] and some scholars have analyzed the application of criminal charges in China. [3]

By analyzing the defects of relevant laws and regulations in China, this paper sorted out the practical obstacles such as the lack of typed awareness of network service providers in China, the failure of systematic and hierarchical laws and regulations, and the disunity of criminal liability determination standards. Based on the analysis of the above problems, this paper puts forward some suggestions to solve the problems in the third part. First of all, it emphasizes that Chinese laws and regulations need to distinguish different types of network service providers, draw lessons from the experience of the German legal system, distinguish different types according to their functions, and achieve an effective path of conviction of network service providers through accurate types of network service providers. Secondly, it makes a comprehensive evaluation of the help behavior of network service providers and gives a limited explanation to the crime of helping information network crime. Thirdly, the refusal to perform the information network security management obligations of the behavior of strict control, emphasis on the fault of the crime in terms of fault requirements, and help information network crime. The last but not least, the relevant legal provisions on the obligations of network service providers should be perfected in the aspects of obligation differentiation and protection of individual rights and interests.

## 2. Practical barriers to sentencing for ISPs

In today's era, the rapid development of information network technologies such as the network, big data, and cloud computing has brought earth-shaking changes to society, and the contact information between social subjects is no longer simple and limited but has become more complex and multi-directional. That means the social activities of "one person to one" and "one person to many people (a few people)" in traditional society have completed the transformation to a new type which now is "one person to multitude ", "multitude to one person" and "multitude to multitude" social activities. The development of information network technology and the enrichment of network services will gradually promote the era of comprehensive informatization and networking of the whole human society. The transformation and development of social relations, accompanied by the reality of lagging legislation, provides a breeding ground for illegal crimes in the field of network. [4] The current cybercrime is rampant and the spread of violence, terror, pornography in this online grey zone cannot be eradicated. The online gambling and fraud are common. What's more, copyright infringement and infringement of personal are also emerging in an endlessly.

It can be seen throughout the entire chain of cybercrime that the status of network service providers in crime chain is crucial because the technical support they provide and their assistance behaviour have obvious characteristics of the criminal industry chain behaviour. In most cases, the existence of network service providers is not attributed to a specific downstream crime but they provide services for many potential downstream network crimes for themselves advantages, which means they are independent. The particularity of the status of network service providers in cybercrime inspires us to start from it to find way to punish cybercrime. Because of their control status and technical conditions, they can better curb the further expansion of the harm of criminal acts, regulate network order, and taking network service providers as the starting point of research is also the consensus of the world's general criminal rule formulation.

At present, the issue of conviction and sentencing of network service providers in China is still a point of controversy, and there is still a certain lack of problems in determining the degree of responsibility of network service providers and measuring the balance between the particularity of the network service providers and the punishment of cybercrime. Taking "Qvod case" as an example, the authors summarize the following problems existing in the judicial practice of conviction and sentencing of network service providers:

### 2.1. The theoretical basis of criminal punishment

Founded in 2007, the main business of the company named Qvod Player is based on streaming media playback technology, through the release of free QVOD server installers and quick broadcast player software to the network, to provide network video services for network users. During the period, the company and its directly responsible executives, for the purpose of profit, knowing that the above-mentioned QVOD media server installer and the Qvod Player were used by network users to publish, search, download and play obscene videos, still allowed them to do these things, resulting in a large number of obscene videos spreading on the network. In the first-instance judgment of this case, the court convicted the defendant, Shenzhen QVOD Technology CO.LTD., of the crime of spreading obscene materials for profit, and convicted the personnel involved in the case of the crime of spreading obscene materials for profit. In this case, the procuratorate's idea of complaint was that the Qvod Player company and its directly responsible supervisors helped users to publish and disseminate obscene videos, constituting a helper for the crime of spreading obscene materials for profit. In the judgment of the judicial organ on the crime of aiding crime of express broadcasting company, the elaboration is vague, and there is still a great gap between the academic circles and judicial practice.

### 2.2. Unclear division of responsibility boundary and identification standard

From the procuratorate's idea of complaint, there is no sufficient evidence to determine Qvod as an accessory. Qvod and its executives do not constitute subjective ideas required by a joint offence. "In terms of joint criminal liability, a path to prosecute network service providers for their criminal liability shall not be limited to prove their general 'knowledge', but there shall be evidence proving their specific 'knowledge'". Therefore, Qvod constitutes an accessory only when the company clearly learns that a specific user releases an obscene video and provides the user with software support. It should be noted that there is a causal link in a behaviour chain. Only when Qvod has the intention to offer help can it be identified as an accessory. However, in this case, there is no sufficient evidence to prove Qvod's subjective elements.

In China's conviction and sentencing of network service providers, standards for determining the degree of responsibility fail to consider subject particularity, that is, work attributes in network service providers. For instance, the standards often centre on whether they are in the "knowledge" of a criminal offence in identifying the crime of assisting criminal activities on an information network. [5] However, insufficient consideration on specific behaviour patterns stipulated in the statutory provision sometimes leads to enlargement of a network service provider's responsibility, which downgrades the modest and restrained principle of the Criminal Law. China lacks a set of systematic logical thinking in the conviction and sentencing of network service providers. [6] It is inevitable to leverage the Criminal Law mechanically in judicial practice, resulting in continuous disputes over judicial cases in this field and greatly reduces judicial efficiency.

### 2.3. The plight of specific application of articles 286.1 and 287 bis of China's current criminal law

#### 2.3.1 The obstacles of the crime of refusing to perform network security management obligations

The judgment standard of subjective states is vague. In the "notice-delete" rule, after the notice is issued, if there is other evidence and facts, it can be determined that the network service provider is subjectively aware and should have known, it needs to bear tort liability. In practice, there is no unified judgment standard and judges have a large space for discretion, so it is necessary to adopt objective standards to help judgment. In the "Qvod case", it is unreasonable to impose "detection obligation" on access software providers. In the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection issued in 2013, obligation of network service providers to manage their contents is stipulated. In this specification, there is no provision on obligation of network service providers to take initiative to review contents, but the obligation to stop illegal information after it is notices. [7] Besides, it is impractical for access software providers among network service providers to completely review user information technically. Time consumed and financial costs are overburdened for enterprises in operation. Moreover, there is certain contradiction between review of user information and individual domination of civil freedom and rights. [8] Hence, it is groundless for procuratorate to "expect" Qvod to review information in advance when there is no provision explicitly stipulated.

#### 2.3.2 The obstacles of the crime of helping cybercrime

Firstly, concurrence between crime of aiding information network crime and other crimes. Through the observation of judicial cases in recent years, it can be found that although there are many cases applicable to this crime, there are few cases directly applicable to this law, which also reflects the problem of cooperation between the crime of helping information network activities and other crimes. For instance, this crime in the judicial application and refused to perform the obligation of information network security management of crime, the crime of illegal use of information network to protect the same social benefits, thus it has the similar information network responsibility, such as the normal operation of maintenance network, take the initiative to report their findings to the regulators of related illegal behaviour, positive cut off the spread of some illegal crime information,

etc., and they all have the same subjective criteria. In addition, traditional crimes carried out by network also lead to confusion in the identification of help information network crime.

Secondly, the criteria for serious circumstances are unclear. Abstract expressions such as "causing serious consequences", "serious circumstances" and "having other serious circumstances" are used in this article. Such expressions are too vague and there is no exact standard such as amount, which may lead to arbitrariness in the determination of criminal responsibility.

To summarize, “Core issue on duty allocation for network service providers lies in an ambiguous distinction between their action and omission, as well as their obligation source of omission and boundaries.” Nevertheless, 2 major issues on duty allocation for network service providers reflected in the main point of dispute over the Qvod case remain unsettled as crime and punishment of network service providers are adjusted in the Criminal Law of the People's Republic of China to date. [9] In judicial practice, there is a general situation that interpretation of a judgment made by a judicial organ is vaguely, and theoretical interpretation in the academic circle varies. In addition, insufficient explanation of the theoretical basis of criminal punishment, ambiguous boundaries of responsibilities and vague identification standards lead to ambiguity and deviations in convicting and sentencing network service providers in terms of cybercrimes.

## 3. Cause analysis

### 3.1 Network service providers are broadly defined in China, which leads to lacks of categorized cognition and application

China has prepared a series of laws, regulations and departmental rules to regulate network since mid-1990s such as the Regulation on network Information Service of the People's Republic of China, the Measures on the Administration of the Publication of Audio-Visual Programs through network or Other Information Network, the Provisions on the Technical Measures for the Protection of the Security of the network, the Provisions on the Administration of network Audio-Visual Program Service, the Interim Provisions on the Administration of network Culture, the Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks, the Amendment (XI) to the Criminal Law of the People's Republic of China, the Data Security Law of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China. [10] However, provisions in the Chinese laws on network service providers are still not concrete or categorized to date.

In Article 287-2 of the Criminal Law of the People's Republic of China, although a specific behaviour pattern is stipulated in the provision, there is no specific constitute condition based on severity and complexity for these different types of services. [11] In addition, the provision offers a one-size-fits-all punishment for these different categories of services in terms of the crime, which is not conducive to the specific application of the statutory provision in judicial practice.

In China’s laws and regulations, administrative regulations and judicial interpretation, specific definition of and recognition on categorization of network service providers are insufficient, and concept of network service providers is determined broadly, which means that “network service provider” is an umbrella term based on which direct responsibility partition is inevitably inattentive. [12] Broad and umbrella features of the concept of network service provider determine its further categorization, so as to precisely demarcate responsibilities of network service providers.

Germany precisely categorizes network service providers, which China can refer to. The Telemedia Act approved in Germany in 2007 basically adopts the Telecommunications Act and the Electronic Commerce Directive. They clarify distinctions among 4 categories of network service providers including network service providers in Article 7, information transfer service providers or channel service providers in Article 8, provisional and automatic cache service providers in Article 9 and storage service providers in Article 10. [13] In the German laws, there are clear classification basis and concept definition for different categories of network service providers, which positively contributes to the conviction and sentencing of network service providers.

### 3.2 Challenges brought by the development of science and technology

The world of technology is aptly called a "technological cocoon" -- the cocoon humans have woven for themselves. In the "technological cocoon" of cyberspace, people may engage in both legal and illegal behaviours, depending on the purpose of the actors. It is the premise of effective criminal substantive law regulation to classify these illegal acts accurately and properly bring them into the criminal circle. Due to the rapid progress of network science and technology, China's criminal law has failed to complete the unified and effective classification of cybercrimes. [14] The difficulty of the classification of cybercrimes lies in that it is not a single criminal activity with distinct individual characteristics, but a collection of various kinds of illegal behaviours in the network space. China's criminal law has not been able to carry out a unified classification of network crimes, most of the classification methods in the academic circle because of the rapid change of network technology and showed limitations.

Therefore, a close observation of China's criminal law can be found that China's criminal law is unable to regulate the risk of scientific and technological innovation due to the "limitations of statutory legislation" and "constraints of the principle of statutory punishment". [15] At present, the existing concept of regulation, focusing on scientific and technological innovation priority means rejecting the intervention of criminal law, and the priority of criminal law regulation will also restrict the development of science and technology, so the balance between scientific and technological innovation and criminal law intervention point becomes the key to solve this problem correctly.

## 4. Solutions

### 4.1 To recognize network service providers in categories

The author believes that the types of subjects categorized according to technology (content providers, access service providers, cache service providers, storage service providers) in German and EU laws and their corresponding exemption standards are worth learning from. This type of quartering model starts from the technical rationality and possibility, aims to limit the responsibility boundary of network service providers and strives to seek sufficient space and clear force boundary for information freedom and media freedom; thus, a proper balance can be found between network security and freedom protection. Through the precise categorization of network service providers, an effective conviction path of network service providers can be realized. In judicial practice, the first step should be judging the types of network service providers, and their behavior characteristics and exemption difficulty that can be involved should be fully understood, after which a qualitative analysis should be conducted on the behavior of network service providers according to the subjective intentional content, the degree of intention connection, the status and action in joint crime, etc., and the criminal charges of network service providers can be finally determined.

#### 4.1.1 Criminal liability of network content service providers

Specifically, according to the Provisions of The German Telecommunications Media Law, content service providers are not different from general criminal liability subjects, and they need to take full responsibility for the content they provide. ICP is defined in Chinese network Information Service Management Measures as a service provider providing information to users through the network. It can be divided into for-profit service providers and non-profit service providers. For-profit content providers mainly generate revenue by creating web pages, advertising, hosting, and providing specific information content. Non-profit content providers are mainly the websites of government departments at all levels, all kinds of public welfare websites of enterprises and institutions, electronic newspapers and periodicals of news organizations, etc.

Network content providers have the right to edit their information, and should review and verify their own information as well as the text, photos and software of the third party. Its criminal responsibility can be divided into two types: one is the information itself constitutes a crime. In theory and judicatory practice, it is agreed that criminal responsibility should be investigated. In this case,

ICP is the direct perpetrator of the crime and should be investigated for criminal responsibility. For example, on the network to publish obscene information, reach the standard of crime constitutes the dissemination of obscene information crime. Second, ICP is helpful to network information. At this point, whether ICP is a crime depends on the circumstances. If it knows clearly that network users are engaged in criminal activities, but still helps them to release and disseminate information, it constitutes a joint crime; If the content provided by the third party violates relevant legal interests, ICP cannot constitute an accomplice in the sense of extreme follower theory. However, whether unilateral accomplice is established needs further analysis. If ICP releases and disseminates the information without knowing that the content of user information is illegal, it is not a crime due to the lack of subjective constituent elements of crime.

### 4.1.2 Criminal liability of network Access Service Providers

network access service providers generally provide routing, optical cable, main network and other technical facilities and basic services of accessing. At present, China's network access service providers are mainly China Unicom, China Mobile, China Telecom and cable TV companies. The dial-up network access, broadband network access and cable TV network access services they provide are network access services.

Access service provider mainly provide a pure transmission service. So, as long as it doesn't transmit first, choose the recipient, change the content, or prior conspire with others to take illegal acts, it shouldn't take the responsibilities for its transmission and the contents. IAP only provides a channel for data transmission, much like a phone company, except that it allows network users to connect to the network through dedicated lines or regular telephone lines. In telephone crime, the perpetrator commits a crime through telephone, and the telephone company does not need to bear criminal responsibility for its legitimate business behavior of providing telephone connection service. Similarly, network access service providers do not have to bear criminal liability for crimes committed through the network due to their legitimate business behavior of network access. Network access service providers do not organize or edit the content of network information, nor undertake the responsibility of review, and do not have the ability to prevent harmful social consequences.

### 4.1.3 Criminal liability of network cache and storage service providers

Stipulated in article 9 of German Telecommunication Media Law in 2007, the cache service provider specified in this article refers to the one that provides automatic and time-limited caching, and this caching only serves to transmit the external information based on the user's request more efficiently. For this independent type of cache service provider, when it recognizes or is notified of the existence of illegal content, it has the obligation to delete and block the illegal content. Failure to comply with this obligation in a timely manner will result in corresponding liability.

Storage service provider stores a certain amount of data information for a long time, and the nature and content of the information remain stable within the corresponding time range, so the provider has a high regulatory obligation on the stored information, and should take the initiative to examine the legitimacy of the information. In the case that the service provider does not have explicit collusion with the criminal, if the illegal information results in criminal consequences due to the service provider's failure to fulfill its duty of review, the provider shall bear the corresponding criminal responsibility for the consequences and be identified as a crime of omission. In the case that the service provider and the criminal clearly conspire, it should be identified as the joint crime of the corresponding crime, and the criminal responsibility should be confirmed by the traditional theory of accomplice.

## 4.2 To comprehensively evaluate the helping behavior of network service providers, and limit the interpretation of the crime of helping information network crimes

Although the active helping behavior of network service providers can be regulated by limiting accomplice theory, it still takes time for the theory to be implemented in China. Moreover, since the

amendment has just been published, the proposal to delete the new article violates the stability of the law and does not have feasibility.

Accordingly, the author puts forward the following suggestions: on the one hand, the concurrence between the crime and the principal crime under various judicial interpretations should be dealt with, and the behavior of network service providers should be comprehensively considered. The force of helping behavior in constituting the principal crime and joint principal crime or joint crime, the daily nature of behavior and the sufficiency of obligation performance should be comprehensively analyzed, based on which the conviction and sentence can be determined. On the other hand, interpretation of helping crime should be limited. Only when the wrongfulness of the act is serious and the network service providers are responsible for the wrongfulness can it constitute this crime. In terms of the regulations about heavier punishment for concurrence, the author believes that this article should be limited and interpreted, and the penalties on network service providers should not be increased. The phrase "simultaneously constituting other crimes" in Paragraph 3, Part 2 in Article 287, should be limited to crimes with a statutory penalty higher than the fixed-term imprisonment of not more than three years, criminal detention or public surveillance specified in the Paragraph 1, excluding crimes lower than the penalty. In addition, it should be pointed out that according to the first paragraph of this Article, the constitutive elements of the principal crime include "knowing + helping + serious circumstances". The penalties for network service providers, who are business behavior providers, should be limited, thus the legislation has made provisions on the seriousness of circumstances, which also reflects the consideration of neutral behavior in the legislation. The author holds that the seriousness of the circumstances not only includes the seriousness of the wrongfulness of the helping act, but also requires the network service providers themselves to be responsible for the serious circumstances. For example, the situations that should be analyzed include whether the help offered to users obviously exceeds their business scope, whether the charge is significantly higher than the market price, or the number and duration of infringing works that they help to transmit, etc.

### 4.3 To strictly control the behavior of refusing to perform the obligation of information network security management, and emphasize the fault requirements

In view of the situation of the loss of evidence in criminal cases in Item 3, the restriction of "seriously hindering the judicial organ from investigating the crime according to law" can be added in practical application to make the application of this article more specific. [16] The author suggests that the formal review obligation of network service providers in the judgment of illegality should be clarified by referring to the clear provisions on the notice of obligees in Administrative Protection of Copyright on the network Procedures. According to the provisions of Articles 5, 6 and 7 of this administrative regulation, the copyright owners have the right to notify the network service providers to deal with the infringing content, but at the same time of the notification, they must submit "copyright ownership certificate, identity certificate and relevant evidence of infringement of the suspected infringing content", etc. Meanwhile, it also stipulates the "counter-notification content" provided by the persons who are accused. Under the above provisions, the network service providers only need to bear the formal review obligation and operate according to the materials provided by the notifiers or counter-notifiers in accordance with the law, and this civil formal review obligation will not constitute the source of obligation of the network service providers in the criminal law.

### 4.4 Further clarify and improve the relevant legal provisions on the obligations of network service providers

Telecommunications Act approved in Germany in 1997 regulates that the service provider shall bear responsibility for the content of the information, at the same time, demands it to bear obligation to the blockade of the illegal content information of others, but, if it meets the "unknown content" "technology could prevent" "resistance is less than its ability to" three conditions, it will be removed from the legal responsibility. Service providers that only "provide access to (illegal content information)" or "automatically cache (illegal content information)" is not subject to regulatory

obligations. The United States Code exempts service providers from civil liability under certain conditions. Compared with information developed countries in Europe and the United States, China's laws and regulations on the obligations of network service providers have the following shortcomings: China's laws are not sufficiently typed for network service providers, only administrative regulations and departmental rules classify network service providers, and there is almost no difference in their management obligations; China's legislation does not stipulate the compensation or payment of ISP's assistance in management, but sets the scope of their assistance obligation too broad, and does not fully protect the relevant rights of the public. China should draw lessons from relevant foreign legislation to set up management obligations reasonably and promote the classification, differentiation and appropriateness of relevant legislation.

### 4.4.1 Stipulate the duty of differentiated management

Intermediate service providers should not undertake the management obligations of managing discovered illegal information and actively reviewing information containing terrorist and extremist content, because such obligations exceed the reasonable scope of their business activities. All kinds of network service providers should not undertake the management obligation of actively reviewing information containing terrorist and extremist content, because assuming such obligation will inevitably lead to the examination of users' secret information and monitoring of information activities, which will seriously undermine the mutual trust between network service providers and users. At the same time, the rapidly increasing amount of information will make the cost of fulfilling this obligation huge and seriously hinder the normal business activities of network service providers.

Network trading platform service providers need to add management obligations. At present, the network transaction platform to a serious shortage of the service provider's management obligation, due to the lack of economic activity network trading platform service provider's safety management is leading to the current network economy, the financial sector fraud crime is one of the important reasons for the flood, so should be set to online trading platform service provider that can meet the needs of its social status and capacity management obligations. Differentiated management obligation is an important embodiment of the scientific nature of legislation.

### 4.4.2 Improve the channels for individuals to appeal their legitimate rights and interests

Making clear restrictions on the sources of obligations of network service providers in the criminal law is only limited to the cases where the regulatory authorities order the network service providers to act and the refusal of the network service providers conforms to the legal circumstances. It requires that in other fields, the ways for obligees to protect their rights should be improved. In addition, the obligations of act arising from the obligees' application and the obligations of act arising from the refusal to perform administrative responsibilities should be distinguished. [17] In the situation of not acting the obligees' act obligation, the network service providers may have a civil tort to the obligees and bear the liability for compensation, which, however, cannot be the premise of criminal liability. In addition, the specific application of this law should be further adjusted according to the problems encountered in practice.

## 5. Conclusions

Due to the unclear definition of the types of network service providers in China's laws and regulations, there are many problems in China's judicial practice such as inconsistent standards for the determination of criminal responsibility and inappropriate application of laws, and there are also many disputes in the academic circle on the sentencing of network service providers. Existing researches on the criminal liability of ISPs mostly focus on the theoretical basis of crime setting and the responsibility of ISPs themselves lacking the combination adjustment of criminal charges and subject typification, as well as restrictions on ISPs' management obligations. Therefore, the paper is based on the current juridical practice and the sentencing barriers of network service provider in China. Combined with legal systems of Germany, the US and other countries, this paper combs out the

possible causes of the problem. On the basis of different types of network service provider, this paper absorbs advanced experience to give suggestions on clearing the path of conviction of network service providers and improving relevant regulations. This paper, for the first time, puts forward a systematic and hierarchical view of regulating criminal liability in the sentencing of network service providers, innovatively proposes solutions such as restricting and distinguishing the management obligations of network service providers and improving the channels for protecting individual rights and interests.

## References

[1] Yang Caixia. Thinking on the Categorization of Criminal Liability of network Service Providers [J]. Law, 2018, 6(4):162-172.

[2] Deng Jinting. Classification of criminal assistance in Cyberspace -- Inspiration from Judicial Decisions [J]. Chinese Journal of Law, 2019, 6(4):138-156.

[3] Wang Wenhua. Application analysis of crime of refusing to perform information network security management obligations [J]. People's Procuratorate, 2016, 24(6):24-27.

[4] Yu Chong. Demarcation of criminal liability for omission of network service providers from the perspective of "dichotomy" [J]. Contemporary Law, 2019, 6(5):13-26.

[5] Zhang Hui. Research on legal application of charges related to cybercrime [J]. Modern Law, 2019, 6(4):156-167.

[6] Chen Hongbin. On the criminal boundary of technology-neutral behaviour [J]. Journal of Nantong University (Social Science Edition), 2019, 6(1):58-65.

[7] Wang Huawei. Identification path of Criminal liability of network Service Providers -- Also comment on the related disputes of Qvod Case [J]. Journal of National Procuratorial College, 2017, 6(5):3-32+173.

[8] Pi Yong. On the management obligation and criminal responsibility of network Service Providers [J]. Studies in law and business, 2017, 6(5):14-25.

[9] Wang Ying. Research on the Attribution model of Network information crime [J]. Peking University Law Journal, 2018, 6 (5):1302-1323.

[10] Qi Wenyuan, Liu Yang. Criminal Law regulation of Network platform providers [J]. Law Science, 2017, 6(3):106-114.

[11] Xie Wangyuan. On the crime of refusing to perform information network security management obligations [J]. China Legal Science, 2017, 6(2) :238-255.

[12] Liu Yanhong. Innocent QVOd and Guilty Thinking -- Reflection and criticism on the theory of guilt in "Qvod Case" [J]. Politics and Law, 2016, 12(12):104-112.

[13] Wang Huawei. Comparative study on criminal Liability of network Service Providers [J]. Global Law Review, 2016, 12(4):41-56.

[14] Tu Longke. Online content management obligations and criminal liability of network service providers [J]. Law review, 2016, 6(3): 66-73.

[15] Guo Zeqian, Zhang Man. A Preliminary Study on the Criminal Responsibility of network Service Providers -- Centered on the punishment of neutral Helping Behaviour [J]. Research on Juvenile Delinquency Prevention, 2016, 6(2):74-84.

[16] Lu Xu. Criminal liability and development of network service providers -- Comments on the relevant provisions of The Criminal Law Amendment (ix) [J]. Rule of Law Studies, 2015, 6(6):61-67.

[17] Tu Longke. Criminal liability model of network service providers and its relationship analysis [J]. Politics and Law, 2016, 6(4):108-115.