



# Definition of “Knowing” of Internet Service Providers in Helping Cybercrime

Haozhe Cheng<sup>1</sup>(✉), Peiwen Li<sup>2</sup>, and Shuyang Li<sup>3</sup>

<sup>1</sup> Faculty of Law, Jiangnan University, Wuhan 430000, China  
ChengHaozhe@stu.jhun.edu.cn

<sup>2</sup> Faculty of Law, Taiyuan University of Science and Technology, Taiyuan 030024, China

<sup>3</sup> Faculty of Law, Hainan Normal University, Haikou 571127, China

**Abstract.** Accomplishing the crime of helping information network crime requires subjective “knowing”. However, since judges cannot explore the inner truth of each perpetrator, there is still a dilemma of confusion in the identification of the subjective state of network service providers. Even in judicial practice, there are a lot of examples concerning the different judgments for the similar cases. This paper holds that the reason for the dilemma of network service providers’ knowing is that under the background of “risk society”, the neutral helping behavior of network service providers who are not “knowing” should not be punishable, but there is no objective condition to assist the identification of whether the actor’s subjective state is “knowing”. On this basis, according to the relevant contents of Article 11 of the Interpretation of Information Network Crime, the judgment standard of “knowing” is put forward, and it is demonstrated by combining with Chinese judicial cases. At the same time, referring to the “neutral helping behavior” in German criminal law, this paper puts forward that the judgment of “knowing” should be based on the principle of subjective and objective analysis, which provides a judgment idea for helping the “knowing” in information network crimes.

**Keywords:** Neutral helping behavior · Subjective elements · crime of helping information network crime

## 1 Introduction

In the context of the information network era, the technical support provided by information network service providers has played an objective role in helping information network criminal activities. It is precisely because of the appearance of neutral legitimacy of the act that some criminal suspects use this as an excuse to request the application of liability exemption, which makes the criminal act complete the transformation from illegal to legal. Therefore, it is of great significance to clarify the constitutive standards of network neutral helping behavior for rectifying the network order, combating illegal crimes and maintaining judicial authority.

---

Haozhe Cheng, Peiwen Li and Shuyang Li—contribute equally.

© The Author(s) 2022

G. Ali et al. (Eds.): ISEMSS 2022, ASSEHR 687, pp. 3645–3655, 2022.

[https://doi.org/10.2991/978-2-494069-31-2\\_427](https://doi.org/10.2991/978-2-494069-31-2_427)

At present, the academia has carried out relevant research on the identification of “knowing” in cybercrime. These researches mainly involve three kinds of methods. Firstly, this paper will analyse objective facts to directly prove the existence of “knowing”. For example, these internet service providers used to receive rectification notice, warning, administrative punishment from administrative department. Perhaps there are network users who have conducted rights protection. Meanwhile, the network service provider’s own security monitoring system has recorded a large number of illegal information anomalies. Secondly, some scholars point out that relying on criminal presumption to identify the existence of “knowing” is a feasible way. If the fact that other people commit violations is like a bright red flag standing in front of the network service provider, it can be inferred that the network service provider cannot fail to find the violations committed by others. That is to say, it can be identified that the network service provider subjectively has a clear understanding [1]. Thirdly, we should allow the perpetrator to submit “counterevidence” to overthrow the previous ones. The degree of proof only needs to reach the level to prove that it is a normal business behavior, rather than requiring the criminal suspect to show they are indeed deceived by others [2].

Through the method of comparative law research, this article will further analyse the recognition rules of “knowing” in order to be directly applied to the practice field.

## **2 Current Situation and Predicament**

### **2.1 Conviction Determination of Network Neutral Helping in China**

At present, the theoretical circle’s identification of the crime constitution of network neutral helping behavior is mainly subjective, objective and compromise. Subjectively, the core of the crime of network neutral helping lies in whether the perpetrator subjectively has criminal intent. Objectively, it is argued that only when the perpetrator creates an impermissible danger and realizes it, can he be held accountable for helping the offender [3]. As for the compromised theory, it requires that the perpetrator not only subjectively has criminal intention, but also objectively creates an unacceptable risk.

In Chinese judicial practice, the conviction of network neutral helping behavior mainly adopts the subjective theory. For example, referring to the clause of crime of helping information network crime, the conviction criteria of information network service providers are analyzed according to the four elements of crime constitution. Firstly, information network service providers objectively provide technical support for cybercrime, which is in line with the objective aspects of crime constitution. Secondly, in the practice, most technical supports provided by network service providers are used by information network criminals. These acts disturb the social public order and constitute the object of crime. Ultimately, the subjective intent of the perpetrator determines whether the provider’s neutral helping can constitute the crime of helping information network crime. In other words, the judge needs to analyse whether the perpetrator has the intention of knowing.

## 2.2 The Dilemma of “Knowing” Identification

### 2.2.1 Different Judgments on Similar Cases in Judicial Practice

In 2007, the Rapid-Broadcasting Technology Co., Ltd [4] deployed its own central scheduling server to build a comprehensive network platform. This website encompasses the functions of publication, search, download, storage and viewing. However, 29841 video files were extracted from the servers hosted by the rapid-broadcasting company seized by the relevant departments for identification, of which 21251 were obscene. Finally, the court found that the four defendants knew that this company provided audio-visual programs containing pornographic content without authorization. Besides, they also allowed these pornographic videos to be stored and downloaded in the cache server controlled and managed by their company. This leads to a large number of pornographic videos spreading on the Internet, which constitutes the crime of spreading pornographic articles for profit. As a result, a large number of pornographic videos were spread online, constituting the crime of spreading pornography for profit.

In another case [5], the defendant, Jin Ziyong, developed a software called Winny that used P2P technology for file information sharing, and also constructed a network platform open to the public. It has the functions of clustering, multiple downloads, and automatic downloads to improve the efficiency of file retrieval and transmission. Two inmates used Winny software to let an unspecified majority access and download software and films on this platform. However, this conduct was lack of legal permission and the consent of the aboriginal author. In other words, they violated the right of the aboriginal author to public communication. However, in Winny’s second and third instance judgements, Jin Ziyong was acquitted from the defendant’s lack of subjective intent [6].

The common point of the two cases is that the information network provided by network service providers has played an objective role in helping criminal activities. However, according to the judgment of subjective intention, it determines whether the objective helping behavior is guilty.

However, what is worth mentioning is that these two cases still involve some specific different points. In the rapid-broadcasting case, the court found that the rapid-broadcasting company had not taken impediments and fulfilled its regulatory obligations, which indirectly helped spread pornographic videos, so as to meet the standard of criminalization. The judgment method of “knowing” is as follows. Firstly, due to the service characteristics of network video platform, fast broadcasting companies should be aware of the possibility that the video websites they provide are used to disseminate pornographic videos according to basic industry experience, relevant industry laws and regulations. Secondly, rapid-broadcasting company has twice been subjected to administrative penalties for failing to implement its regulatory responsibilities and for the presence of a large number of pornographic videos in the Broadcasting Network. That is to say, this corporation has received clear notification from the administrative authorities. Thirdly, some obscene videos are automatically stored by the cache server due to the high number of users on demand and downloads. As a network service provider, it is impossible for the fast broadcast company to not know the high-demand and downloaded video content in the server it provides.

In Winny's case, the court's requirement that persons reaching the non-exceptional scope use the software to commit a criminal act is highly probable. Besides, it is understood and tolerated by the provider. Under this condition, it constitutes subjective intent to induce others to use it illegally. From the defendant's subjective point of view, it can be found that the defendant is aware of the fact that there are some people using Winny to violate the indigenous right of others and the number of these people is increasing when publicly providing the Winny of this case. However, nowadays, there is no evidence to prove that the defendant providing this software can understand and tolerate such facts. For example, the use of Winny leads to infringement of indigenous rights to expand to the non-exception range, meanwhile, the scope of the implementation of indigenous rights infringement probability is higher [7].

### 2.2.2 The Dilemma of "Knowing" Identification

Observing the judicial cases of various types of cybercrimes, it is not an obstacle to find that in terms of some cybercrimes, there is no need for two-way intentional contact between the helper and the principal offender. The criminal behavior of helping cyber information can be implemented. The helper only needs to publish specific information through the network platform, while the perpetrator can obtain them. There is no need for meaningful communication between these two parties [8]. This brings a lot of problems to provide evidence to prove subjective intention. At present, the theoretical circles even vividly divide these one-way intentional contacts into "indifference" separate radial cybercrime and "carelessness" chain cybercrime [9]. The former information network crime helper belongs to the neutral helping behavior. It means that it can be used to provide normal network services, but also can be used to help the implementation of crime behavior. Therefore, many helpers always refuse to admit the crime of helping on the ground of "unknowing" when defending themselves so as to evade criminal responsibility. In the whole "industrial chain", the latter part of the helpers is located at a very small part of the link. Additionally, due to the lack of meaning contact, these helpers even do not know their upstream and downstream links and their own roles in the whole practice. However, these helpers can have a certain understanding of the helping role of their own links, and it is obviously unreasonable not to assume responsibility. Therefore, for them, the subjective punishability also falls on the helpers' cognition of their own helping behaviors. These practical difficulties have brought great challenges to the judicial organs in terms of subjective identification.

## 3 Causes of Difficulties

### 3.1 More Difficulties for Providers to Supervise in the Information Age

There is a theory of "risk society" [10] in the field of sociology. It refers to the social development stage in which the global risks caused by human practice dominate under the background of globalization. In such a society, various global risks pose a serious threat to human survival and development. The author believes that this is also the reason for the confusion of how to identify if the accomplice is subjective "knowing". With the rapid development of the Internet, more and more users use the network platform

to release information. While enjoying the convenience brought by the information network, personal information is inevitably exposed to the “big network” of the Internet and bears security risks. Not only is it difficult for victims to identify, but as a neutral platform provider, network service providers are also unable to prevent various criminal means. In addition, information network crime presents a development trend of black and gray industry interest chain, which provide technical support to the perpetrator of network information crime, and then the perpetrator of information network crime commits crime [11]. For the interlocking “professional” criminal means, it is difficult for network service providers to achieve 100% prevention and control.

In this case, it is obviously unrealistic for network service providers to supervise the use of each user and avoid all illegal acts. This means that the network service provider does not of course have the condition of “knowing”, which undoubtedly increases the difficulty in determining the state of “knowing”.

### 3.2 Lack of Objective Conditions that Can Be Identified as “Knowing”

“Knowing”, as a subjective element, is difficult to define in the constitution of crime. Therefore, for the “knowing” of network service providers, how to identify it with objective conditions is the key to be solved urgently.

First of all, the rapid development of science and technology is indeed a “double-edged sword”, which not only makes us in a risk society, but also gives unprecedented scientific and technological support to human social activities. The introduction of scientific and technological means into case investigation is not unprecedented, such as lie detector and hypnosis technique. Such technical support does exist in China’s criminal technology appraisal department. However, there are two major gaps in such objective material conditions. Firstly, at present, lie detector and other high-tech equipment only exist in criminal technology identification departments, and grass-roots criminal police teams are not equipped with these instruments, that is to say, the supply capacity of high-tech equipment has not yet reached the level of meeting the demand. Secondly, even if the criminal technology identification department has a lie detector, it is only used to assist the investigation, and the test results cannot be directly used as evidence. This is fully in line with humanistic care. The human brain is so complex that using high-tech equipment to judge people’s subjective state cannot be 100% accurate. Using the test results as evidence is inevitably farfetched and violates the principle of “suspected crime comes from nothing”. Therefore, it is not feasible to use only material conditions to supplement the gap of insufficient objective conditions so far.

In contrast, the introduction of judicial interpretation as the standard of conviction is obviously more reasonable. That is to say, we need describe the current effective law from the perspective of legal dogma and put forward suggestions to solve difficult problems in order to standardize practice. Historically, the authority of law is not based on people’s rational research on him, but on the strength of politics. Therefore, the research of law in traditional law is basically based on a deep belief, and there is little critical spirit. Just like the interpretation attitude of Holy Scriptures, legal dogmatics is also classified as an arbitrary dogmatics. Its premise is that the meaning in the literature has long been fixed and clear, there is no need for us to explore it again. It can be seen from this that whether the act of providing neutral helping by network service providers in criminal

law should be recognized, the act of helping network crime should be made a clear legal interpretation, and then a clear interpretation should be used to regulate the practical behavior.

As mentioned above, Article 11 of the interpretation of the Supreme People's court and the Supreme People's Procuratorate on Several Issues concerning the application of law in handling criminal cases such as illegal use of information networks and helping information network criminal activities gives seven judgment criteria from different angles to determine the subjective "knowing" of the perpetrator. For example, the act of providing help after being clearly informed by the relevant departments will be judged as the perpetrator's subjective "knowing". We can judge whether the transaction process is normal by the price. If the transaction price is obviously abnormal, it can be presumed that the perpetrator is in the state of "knowing" subjectively. As for network service providers, paragraph 1 of Article 28 of the Criminal Law Amendment (9) [12] stipulates what consequences network service providers will be punished for failing to perform their regulatory obligations. In addition, according to the paragraph 4 of Article 29, the provider will be punished by the criminal law in a specific situation. The situation is network service provider providing technical support or assistance to others when knowing that others use the information network to commit a crime. Based on the combination of the two, it can be seen that the criminal law stipulates that network service providers do not perform their regulatory obligations or still provide network services for others with the subjective intention of committing a crime, resulting in harmful results. In this regard, some scholars identified the behavior of network service providers providing network services as "neutral helping behavior" [13]. Then whether the behavior of network service providers is punishable should be classified and discussed according to their subjective state.

Citing the fast-broadcasting case and Winny case mentioned above, we can find the fundamental reason for the different judgments in such cases. There is no unified and clear judgment standard for the judgment of "knowing". Different judges will make completely different judgments according to their different cognition and the constraints of other factors. According to the judgment standards of helping behavior of different crimes in the previous criminal law, different helping behaviors have different criminalization standards, and the requirements for the degree of "knowing" of helping criminals are also different. There has not been an authoritative standard for the subjective identification of helping behavior in China's theoretical circles, so it is impossible to directly misappropriate the subjective judgment standards of other helping behaviors in the criminal law to judge the "knowing" of network service providers. Therefore, the lack of targeted judicial interpretation to provide objective conditions for the subjective state of network service providers as the identification standard is the main reason for the confusion of the identification of "knowing" and the different judgments of similar cases.

## 4 Judgment Method of “Knowing”

### 4.1 Defining the Standard of “Knowing”

In the above discussion, we can see that the determination of whether to “help information network crime” is mainly that of “knowing”. Judging whether it belongs to “knowing”, the author believes that it can be judged whether it belongs to “knowing” according to the relevant contents stipulated in Article 11 of the Interpretation of Information Network Crimes.

First of all, it is impossible for the network service platform provider to fully supervise whether all users on their platform have committed criminal acts by using the platform. However, after being informed by the regulatory authorities, it will be judged as “knowing” that the relevant acts are still carried out. Specifically, after being reminded by the relevant departments, the provider ignored its supervision, connives. He or she did not actively cooperate with the users, delays and disputes, and takes “knowing” as an excuse. For example, in the “Pan Mou”, the appellants Pan Mou, Liu Mou, and accessory Zhang Moulun all confessed in the investigation stage. When Pan Mou and Liu Mou sold their bank cards, they knew that the bank cards they sold would be used to commit online gambling, money laundering and other information network crimes. At the same time, when they applied for bank cards, the risk notice of bank account opening also had a clear prompt. Pan and Liu Mou also signed the risk notice for confirmation. Accordingly, the court held that the case file evidence could fully prove the fact that Liu knew that others committed crimes by using the information network, but still provided them with payment and settlement assistance. After the trial, the court held that Pan Mou, knowing that others used the information network to commit crimes, still provided payment and settlement assistance to them. If the circumstances are serious, his behavior has constituted helping the information network to commit crimes [14].

Secondly, if the network service provider fails to perform the statutory management duties after receiving the report, it should set up a report box on its platform, or display the report channels such as the report telephone. When the masses report the illegal and criminal acts of their platform users, the platform service provider should immediately check and report to the relevant departments after knowing. If the platform service provider ignores possible crime report and continues to provide the platform for its use, this is “knowing”.

Thirdly, if the transaction price or mode is obviously abnormal, it mainly means that the provider’s fees are obviously higher than the national standard industry regulations or the payment mode is abnormal. For example, in the case of Hou Zhongxiong, Hou Zhongxiong knew that others used the information network to commit crimes, and provided two bank cards with payment and settlement for his crimes. There were 22 cases of fraud related to two bank cards, and the accumulated capital was 508,405.01 yuan. The court held that if the circumstances were serious, it constituted the crime of assisting criminal activities in information network [15].

Fourthly, the perpetrator provides programs, tools, or other technical assistance that are specifically used for illegal crimes. Under the information environment, the emergence of various platforms and inadequate network supervision have led some lawless

elements to commit crimes by using the network. This article mainly refers to the behavior of some false and fake website providers who cheat people's trust and obtain illegal interests by forging official platforms. Under such conditions, the network service provider constitute "knowing".

Fifthly, we often use means such as hiding the Internet, encrypting communications, destroying data or using false identities to evade supervision or investigation. For example, in the case of "Lin Zhipeng", Lin Zhipeng, Chen Xiangyang and Wang Zhiyi agreed to provide a platform for others to send short messages on the Internet for profit, that is to say, through the website of "International Short Message Channel" with the function of sending short messages, they opened accounts for others, set the number of short messages, and sold them to others at a price of about 0.35 yuan per short message. They also agreed with the channel operators that Chen Xiangyang and others would get a commission of about 0.03 yuan per short message, and the rest of the money would go to their families. Chen Xiangyang was mainly responsible for financial work, Wang Zhiyi was mainly responsible for technical work such as docking channel websites, and Lin Zhipeng was mainly responsible for technical services such as docking customers, with profits shared equally among the three. Chen Xiangyang and others hired Zhu Mingming to do accounting, collection, transfer, withdrawal and other financial work with a monthly salary of 8000 yuan. They collected other people's bank cards for collection, transfer and withdrawal, and use foreign chat software with encryption and data destruction functions to conduct business through SMS channel, thus evading supervision. The court held that Lin Zhipeng knew that others used the information network to commit crimes, but still provided them with advertising and promotion assistance. If the circumstances are serious, his behavior has already constituted a crime of helping the information network [16].

Sixthly, the perpetrator provides technical support and assistance for others to evade supervision or investigation. This article refers to the situation that Internet service provider discover that users use their platform to carry out illegal and criminal activities. At the same time, network service providers continue to provide a platform for users by modifying cover-up data for profit. This kind of behavior is "knowing".

Seventhly, all other behaviors of the actor can be regarded as "knowing". This one has a wide range. The author believes that this article can be judged from the cognitive concept. The concept of "knowing" is very clear, and the conceptual boundary of "knowing" is very important. For example, in the case of "Zhou Moqi and You Mojie", the perpetrator obtained the calling card by illegal means after defrauding students to handle the calling card through false information, and then sold it out of the country. Criminals used it to commit fraud. In this case, Zhou Moqi and You Mojie illegally obtained and sold phone cards. Although the amount and quantity are within the normal range, it was obviously unreasonable to buy and sell, and there were many transactions. Therefore, in this case, the actor's behavior "should know" meant that the condition of "knowing" was met. In the end, the court made a judgment on the crime of helping the criminal activities of information network. The author believes that when judging "should know", the actor's geographical location, professional habits and so on can be used to help the judgment. When the actor was in a special industry, it could be considered that his occupation required him to master relevant laws and regulations, and he



couldn't shirk his legal responsibility with ignorance as an excuse. When the actor was located in a remote area, his knowledge level was limited, and his network usage was extremely unskilled, his behavior could be judged as ignorance.

#### **4.2 Adhere to the Principle of Unity of Subjectivity and Objectivity to Judge Knowledge**

It is a subjective cognition to “knowing” others to commit crimes by using information network. This kind of subjective knowledge is the expectation of network service provider for actual cybercrimes, rather than the knowledge of cybercrimes that have already occurred. This kind of psychological activity cannot be perceived directly [17].

The cognizance of the crime of “knowing” to help information network criminal activities is mainly reflected in judicial practice. It is even more necessary to combine knowledge with practice, and follow the principle of the unity of subject and object. This can learn from the German theory of the combination of subjective and objective, and make a judgment on neutral helping behavior. German Professor Roxin believes that the subjective aspect needs to be judged by the “trust principle”, and the objective aspect needs to have a causal relationship, which can be attributed.

The author believes that adhering to the principle of the unity of subject and object needs to be understood and applied correctly. In judicial practice, it is necessary to fully consider the motive of the actor, analyze whether there is a subjective aspect of intention, and also consider the consequences of his behavior and the objective aspects of specific situation. When the actor is intentional and negligent subjectively, but the objective aspect lacks corresponding harmful result, the principle of unity of subjectivity and objectivity should be adopted to limit it. If it causes harmful consequences objectively but lacks subjective recognition, it is also necessary to use the principle of unity of subject and object to determine whether it constitutes a crime and what crime it constitutes. The principle of combining subjectivity with objectivity provides theoretical helping for understanding the actor's “knowing” from the aspects of behavior, subjective initiative, objective results and so on. For example, in the case of “You Mougou”, the point of dispute between the public prosecutor and the defendant's defender is whether it is a crime of aiding trust. When judging this controversial point, it is particularly important whether you know the specific content and amount of the criminal activities of Haoyou Company. Judging from the principle of unity of subject and object, the online platform of the mall made by You Mougou has been used by other defendants to commit fraud, and its behavior has been in line with the objective aspect of helping the trust crime. In this case, you did not take relevant measures for control and management after receiving specific complaints and asking the website investors for verification, so it can be presumed that you are subjectively informed. Combined with your educational level and cognitive ability, you have done the daily maintenance of the website while knowing that others are using the online shopping mall platform developed by you. Your behavior has already met the subjective aspect of the crime of supporting trust, which is in line with the constitutive elements of the crime of supporting trust. According to the principle of the unity of subjectivity and objectivity, the analysis of cases can provide a clear and normative perspective for judging “knowing”.

## 5 Conclusion

This paper summarizes the core issue, which is how to “recognize” the crime of helping information network. In criminal activities, “knowing” is subjective and hard to judge. At the same time, the neutral helping behavior of network service providers is in the middle zone that is difficult to be directly identified. In this case, “knowing” is even harder to judge. This paper takes the current predicament as the entry point, and lists the different judgment results of two similar cases including the fast broadcast case and the Winny case. At the same time, it deeply analyzes the objective reasons for the confusion of subjective “knowing” determination. The author believes that under the background of “risk society”, Internet service providers can’t control users’ behavior in all directions when providing Internet services. Therefore, the material conditions to support the cognizance of “knowing” are limited, and the judicial interpretation is vacant. On this basis, according to the relevant contents of Article 11 of the Interpretation of Information Network Crime, the judgment standard of “knowing” is put forward, and it is demonstrated by combining with Chinese judicial cases. At the same time, referring to the “neutral helping behavior” in German criminal law, it is proposed that subjective and objective analysis should be taken as the principle to judge “knowing”. It provides a kind of judgment thinking for helping “knowing” in information network crime.

## References

1. Y.L. Sun, Research on the core issues of the crime of helping information network criminal activities, in: *Political and Legal Forum*, Vol. 37, 2019, pp. 80–91.
2. J.P. Huang, Rule judgment in the identification of new cybercrime, in: *Chinese Journal of Criminal Law*, Vol. 06, 2017, pp. 3–13. <https://doi.org/10.19430/j.cnki.3891.2017.06.001>.
3. W.Q. Yao, Neutral helping and objective accountability theory, in: *Jurist*, Vol. 06, 2017, pp. 129–180. <https://doi.org/10.16094/j.cnki.1005-0221.2017.06.011>.
4. Beijing Haidian District People ‘ s Procuratorate of Beijing City v. Shenzhen Fast Broadcast Technology Co., Ltd., Wang Xin, et al., Beijing City First Intermediate People ‘ s Court Case No. 592(2013), Procedure of Second Instance, December 15, 2016.
5. Tokyo Procuratorate v. Jin, Ziyong, Second Criminal Department of the Kyoto Local Court Case, No. 2018/2003, December 30, 2004.
6. Y.C. Wu, Judicial determination of neutral assistance, in: *Judicial Application of Law*, Vol. 12, 2017, pp. 3–10.
7. C.C. Chu, Theoretical deconstruction of restricting network platform helping behavior punishment, in: *Chinese Journal of Criminal Law*, Vol.06, 2017, pp.49–67. <https://doi.org/10.19430/j.cnki.3891.2017.06.005>.
8. Z.G. Yu, The sanction system and improvement idea of criminal helping behavior in cyberspace, in: *Chinese Law*, Vol. 02, 2016, pp. 8–24.
9. S. Jiang, The interpretation direction of the crime of helping information network criminal activities, in: *the Chinese Journal of Criminal Law*, Vol. 05, 2020, pp. 76–93. <https://doi.org/10.19430/j.cnki.3891.2020.05.005>
10. U.Beck, *Risk Society*, Yi Lin Press, 2004.
11. M.L. Li, Research on the inaction responsibility of network service provider in telecom network fraud crime, in: *Journal of Information Security Research*, Vol. 8(2), 2022, pp. 165–171.

12. Amendment to the Criminal Law of the People’s Republic of China (9), 2021.
13. Z.Q. Guo, M. Zhang, A preliminary study on the criminal responsibility of internet service providers: centered on the punishment of neutral helping behavior, in: *Juvenile Delinquency Prevention Research*, vol. 2, 2016, pp. 74–84.
14. Pan and Liu are guilty of helping information network criminal activities, Zunyi City intermediate People’s Court of Guizhou Province Case No.425 (2021), Qian 03, November 18, 2021.
15. Hou Zhongxiong’s Crime of Helping Information Network Crime, Weichu Intermediate People’s Court of Yunnan Province Case No.163, Yun 23 Penalty End (2021), October 28, 2021.
16. Criminal judgment, Lin Zhipeng, the first criminal trial of helping information network crimes, Jiangle County People’s Court of Fujian Province Case No. 94, Min 0428 (2021), September 8, 2021.
17. Z.G. Yu, New Exploration of Cognitive Theory in Criminal Intention, in: *Law Research*, Vol. 30, 2008, pp. 96–109.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

