Science of Law Journal (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2023.021009
ISSN 2616-2296 Vol. 2 Num. 10

Study on the Obligations of the Crime of Refusing to Fulfill the Obligations of Information Network Security Management

Yinshuang Ma

Department of Laws, Dalian Ocean University, Heishijiao Street, Dalian, Liaoning, China
1063633476@qq.com

Keywords: Internet crime; duty of Information Network security management; network service provider

Abstract: With the continuous development of the internet today, the Internet has greatly promoted the progress of society, but its impact also has to attract our attention, the internet crime more and more at the same time the breeding of new forms of crime, so that the traditional criminal law can not be completely regulated, the new law has also solved this problem. The new law is the criminal law amendment (IX). According to the new crime of refusing to implement the regulation of network security management, the network service provider must bear the criminal responsibility for his inaction, which has laid a new legal basis for the security management of network crime. However, there are many problems in this charge, such as the low application rate of the court. This paper focuses on the legal background and judicial system of the crime of failing to perform the responsibility of Information Network security management. Using the general idea of the present situation, the paper puts forward the requirements for information network security, then expounds the existing problems and puts forward remedial measures.

1. Legislative background and judicial application status

From the perspective of traditional criminal law, the traditional charges can not be applied to the new network crime. When the Internet first developed, most of the crimes were computer-related, so the legislature limited itself to computer-related crimes when it set up the relevant charges to protect the security of computer systems, with the development of Internet technology, the protection of data information and the security of non-computer equipment is very important. A single subject often can not constitute an independent network crime, in the network crime there will often be a network service provider involved, to network service users to provide online payment, search engines and other network services, facilitate the completion of a crime. As for the problem that it is difficult to identify the new type of cybercrime in judicial application, we can not simply use the traditional crimes to impute, which will allow the harmfulness of the network spread to further expand, or it is hard to convict and punish Internet service providers for their inaction. Therefore, it is very necessary to add the crime of refusing to fulfill the duty of Information Network security management, which not only further standardizes the omission behavior in the

network crime, but also expands the scope of the attack of the subject of the network crime.

In the search for the keyword “Network security management obligations”, can be seen from the case of the 42 defendants judgment, the development and operation of web sites, applications and other internet-related businesses is the content of the defendant. However, the court did not define in its judgement whether the defendant was a provider of internet services or whether it had violated any of its obligations. The regulatory authorities also ordered a small number of rectification measures, with most being ordered to close down. In the judgment documents of 7 cases convicted and sentenced for the crime of "refusing to fulfill information and network security management obligations", there was no detailed explanation of the defendant's rectification situation. By setting up the crime of refusing to perform the duty of Information Network security management, the legislator restricts the behavior of the network service provider, in order to make it fulfill the duty of network security management. Although network service providers often violate their network security management responsibilities in reality, compared to other online crimes, searching in the network of judicial documents reveals that the applicability of this crime is extremely low. I think there are two reasons for this. On the one hand, when an ISP violates this crime with serious consequences, it can often also constitute other crimes. In other words, this crime is likely to coincide with other crimes, because the legal penalty of this crime is relatively light, when the imaginative concurrence occurs, the choice of a heavy start, it will be convicted of other crimes sentencing, resulting in a low rate of application of the crime. On the other hand, this crime has set up the double obligation for the network service, which makes the threshold of the crime is high and the standard of the crime is vague, which is also a reason of the low application rate of this crime in the judicial judgment.

2. General concept of the obligation to manage the security of information networks

2.1. Sources of information network security management obliga-tions

In the past period of time, relevant laws and regulations on network security management have been relatively lagging behind. Some abstract laws and regulations on network security management are relatively abstract and difficult to operate in practice. The concept of network service providers not fulfilling their information network security management obligations under laws and administrative regulations is difficult to define. This situation has only slowly changed in recent years, and the current relevant laws directly or indirectly provide for network service providers to fulfill the obligations of information network security management stipulated in laws and administrative regulations. The Network Security Law also makes more specific and orderly provisions on the information network security management of network service providers.

2.2. Content of information network security management obligations

1) Failure to perform information network security management obligations

According to article 286-1 of the Criminal Code, this crime is a pure obligation to omission and cannot be constituted by an act, but only by omission. As a typical type of obligation, the network security management obligation involved in this crime is that information network service providers shall perform the obligations of acts and omissions related to information network security management clearly stipulated by current laws and regulations in accordance with law.

2) Refusal to take corrective measures after being ordered to take corrective measures by the regulatory authorities

The crime of refusing to perform information network security management obligations must violate dual obligations to constitute a crime, that is, only the refusal to perform information

network security management obligations is satisfied does not constitute this crime, and it is also necessary to have the act of refusing to make corrections after being ordered to take corrective measures by the regulatory authorities. [1]The legislator specifically stipulates that the standard for establishing a crime is different from that of ordinary obligation-the second layer of obligations, which is to avoid increasing the burden of obligations on network service providers, and to constitute this crime, it is necessary to violate the second layer of obligations on the premise that the network service provider violates the first layer of obligations, and the network service provider's behavior may be evaluated in criminal law before it can constitute this crime. Article 2 of the judicial interpretation issued by the Supreme People's Court and the Supreme People's Procuratorate, "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving the Illegal Use of Information Networks and Assisting Information Network Criminal Activities", clarifies the determination of "refusal to make corrections after being ordered to take corrective measures by the regulatory authorities" in this crime. The first paragraph of Article 8 of the Cybersecurity Law stipulates: "The state internet information department is responsible for the overall planning and coordination of network security efforts and related supervision and management efforts. The competent departments for telecommunications, public security departments, and other relevant organs under the State Council are responsible for network security protection and supervision and management efforts within the scope of their respective duties in accordance with the provisions of this Law and relevant laws and administrative regulations. ” This paper clarifies three problems according to the current situation of law enforcement and judicial practice. First, the scope of regulatory agencies, such as network information, telecommunications, public security and other institutions legally responsible for information network security regulatory duties. The second requirement is that the corrective order must be made in the form of a notice of corrective order or other instrument.[2] In the third step, a comprehensive determination is made as to whether there is a "refusal to correct", and a careful assessment is made as to whether there is a legal or administrative regulatory basis for the supervisory authority's order to correct, whether the necessary corrective measures and deadlines are reasonable and clear, and whether the network service provider has the ability to take corrective measures as required, among other factors.[3]

3. Problems with information network security management obli-gations

3.1. Problems with first-tier obligations

3.1.1. Unclear content and scope of information network security management obligations

There are two problems with the first tier of obligations. On the one hand, ISPs are divided into groups and subject to a variety of complex legal requirements. It is unreasonable for ISPs to be held to the same standards. When legislators establish laws and regulations to set obligations for network service providers, in addition to the need to typify the obligations of network service providers, it is also necessary to set certain principle-based restrictions to underwrite the obligations of network service providers, so as to avoid the expansion of the obligations of network service providers and the imposition of unnecessary burdens on them. At present, the obligation of information network security management provided by network service providers is scattered and abstractly distributed in various laws and regulations in our country, this further creates the problem of indirect citation of blank counts. Under the mechanism of coordinated supervision by various departments, if the boundaries of the obligations of network service providers are not clearly defined in the law, when the government and network service providers fulfill their respective supervisory obligations, problems such as ambiguity in the boundaries of responsibility between the two are likely to arise.

3.1.2. Overgeneralization of the obligation to manage the security of information networks

When an ISP provides network services, its internal or external control over the management of network security may become the subject of scrutiny of the obligation of this offence, giving rise to a normative evaluation of the criminal law. This makes the obligation of the network service provider too broad. Since only partial deviation and loss of control can be regarded as causally related to the result of damage under criminal law, this indirectly limits the scope of the obligation of network service providers. However, the extensive requirements of information network security management impose additional obligations on information network service providers on an abstract level. After all, criminal law is of a modest nature and, therefore, network service providers cannot be held criminally liable in a generalized manner. In addition, any loophole in information network security may lead to problems in the security control of the entire information network, and it is essential to avoid over-generalization of the obligations of network service providers.

3.2. Problems with second-tier obligations

Since the legislation of the crime of refusing to fulfill the duty of Information Network security management, there has been a tendency to reduce criminal punishment. This crime establishes the dual application of administrative law and criminal law, i.e., "ordering correction and refusing to correct".

According to the order of "first administrative and then judicial", the network service provider constitutes this crime will inevitably be affected by the law enforcement of administrative organs, and there are three main problems in the regulatory body of administrative organs. The first is administrative misbehavior. The staff of the administrative organs do not correctly fulfill their duties, do not perform their duties ex officio in accordance with the laws and administrative regulations, resulting in the network regulatory department regulatory dereliction of duty, overstepping the authority, abuse of power, and flaws in the regulatory process, making the regulatory effectiveness extinguished. The second is administrative inaction. Administrative inaction refers to the negative failure of regulatory authorities to fulfill their due regulatory duties, condoning the illegal and criminal problems in the network platform, and not cracking down on the illegal activities in the network. The third is the lack of capacity of the regulatory authorities themselves, with different regulatory authorities passing the buck to each other, leading to poor regulation and loopholes.

4. Methodology for the refinement of the first tier of obligations

4.1. Methodology for the refinement of the first tier of obligati-ons

4.1.1. Distinguishing the regulatory obligations of ISPs

Different types of network service providers should make a typological distinction between different types of obligations. First, for the obligation to retain user information, network service providers should adopt the principle of legitimacy and legality, protect user information, not tamper with it, leak it, or destroy it, and take effective protection measures to avoid information leakage that would lead to the expansion of the crime. Secondly, it is the management obligation of the information released by the user, the network service provider shall have the obligation to review the information released by the user in advance to ensure the safety and legality. If illegal information is found to exist, it should be deleted in a timely manner, and if the user does not delete it immediately, the network service provider should take immediate measures to prevent the further

dissemination of illegal information. Finally, the network service provider's obligation to assist law enforcement. For network service providers, assisting law enforcement is their basic obligation, and they should at all times cooperate with public authorities in combating cybercrime, but within their capacity, and network service providers with dominant capacity should also retain information in a timely manner.

4.1.2. Our laws should create regulatory obligations that are proportionate

Excessive reliance on social control of the Internet would be counterproductive, resulting in damage to the interests of all parties, which requires legislators to find a balance between national interests, social interests and public interests to achieve appropriate legislation. At present, the scope of obligations should also be appropriately limited, not only to limit the types of obligations, but also to exempt network service providers from the relevant legal responsibility, in the network service providers to meet the "informed" "have the ability to organize" and "have the appropriate ability to withstand", "have the appropriate ability to withstand". Only when the network service provider meets the requirements of "being informed", "having the ability to organize" and "having the corresponding ability to bear" should it assume the corresponding legal responsibility. At the same time, the power of users and personal information should also be adequately safeguarded, and the obligation to provide users' personal information and data to national public authorities should be subject to appropriate substantive conditions and legal procedures, and reasonable procedures should be set up for the destruction of users' information and for the relief of users' power.[4]

4.2. Methodology for the refinement of the second tier of obligations

A regulatory order for correction is an administrative order. The whole process of ordering corrective measures means that the administrative supervisory department with law enforcement power monitors the loopholes in network security management, proposes corrective programs for the loopholes, and requires network service providers to carry out corrections in accordance with the given programs. The administrative supervisory department should pay attention to the fact that it cannot be uniform when ordering network service providers to make corrections, and needs to analyze specific problems and give guidance. Firstly, when the administrative supervisory department enforces the law, it should clearly point out to the ISPs what laws have been violated and what kind of obligations they need to fulfill. Secondly, when the administrative supervision department points out the problems of the network service provider and orders it to make corrections, it should inform it of the correct practice, and if it has already had a bad influence, it should actively help it not to further expand its influence. At the same time, specific requirements should be put forward. Third, enforcement should be reasonable. While strictly enforcing the law, the capacity and cost of network service providers should also be taken into account, so as not to impose an excessive burden on network service providers. Finally, it is necessary to ensure that the actual network information security governance does truly minimize risks.

5. Conclusions

First of all, this paper introduces the legislative background and judicial application status of the crime of refusing to fulfill the duty of Information Network security management, this paper analyzes the importance of the crime of refusing to fulfill the duty of Information Network Security to the present network environment governance, and puts forward the reasons for the low judicial application rate of the crime of refusing to fulfill the duty of Information Network Security. Secondly, this paper introduces the general concept of Information Network security obligation,

introduces the source and content of information network security management obligation. Thirdly, this paper introduces the problems of the obligation of information network security management, and puts forward the problems of the obligation of information network security management and supervision from two aspects. Finally, a solution to the existing problems is proposed.

Acknowledgements

I am very grateful to my teacher for my help in writing this paper, I will continue to work hard, use my knowledge, in the field of cyber crime continue to study, live up to the teacher's expectations of me.

References

[1] Zhou Guangquan. Judicial application of the crime of refusing to fulfill the duty of information network security management [J]. People's Procuratorate, 2018(09): 16-22.
[2] Wang Chunhui. An analysis of the ten legal systems and basic characteristics of the cyber security law [J]. China Telecom, 2016(12): 11-16.
[3] Zhou Jiahai, Yu Haisong. Understanding and application of the interpretation on several issues concerning the application of law in criminal cases concerning illegal use of information networks and assistance in criminal activities on information networks [J]. People's Justice, 2019(31) : 25-29. DOI: 10.19684/J. CNKI. 1002-4603.2019.31.007.
[4] Ma Yongchun, Wang Teng. The applicable predicament and relief of the crime of refusing to fulfill the duty of information network security management [J]. Journal of Shandong Police College, 2018, 30(03): 12 -20.