Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/16/20231119

The Application Dilemmas in the Crime of Refusing to Perform the Obligations of Information Security Management

Zhe Pan[1,a,†], and Jingyi Xiong[2,b,*,†]

[1]*Law School of Artificial Intelligence, Shanghai University of Political Science and Law, Shanghai, 201700, China*
[2]*Law School, GuangXi Minzu University, Nanning, 530000, China*
a. wenansama@gmail.com, b. webmaster@gxmzu.edu.cn
**corresponding author*
[†]These authors contributed equally.

Abstract: Aiming at cybercrimes, China has stipulated the crime of refusing to perform the obligations of information security management in the Amendment (IX) to the Criminal Law. However, in judicial practice, the application of this crime is extremely rare, causing a waste of legislative resources. The reason can be attributed to the zombification of legal provisions. This paper focuses on the dilemma of applying this crime in judicial practice. There are two specific dilemmas. The one is the identity of the applicable subject of the crime and the accompanying management obligations are vague. The other is that the boundary Between this crime and the crime of aiding network information crime is unclear, which can be attributed to the similarities in constituent elements. There are three aspects that this paper considers confusing including the identity of knowing, their criminal patterns and the boundaries Between consequential and behavioral offenses. Based on these judicial application dilemmas, this paper urges that the court should consider the details of the cybercrime more carefully in the trial to better apply this crime. Meanwhile, it is unacceptable to directly apply the crime of aiding network information crime as a pocket crime without detailed analysis. The popularization of law should focus on the underlying logic, which means targeting netizens. Therefore, the ultimate goal of eradicating cybercrime can be achieved.

Keywords: judicial application dilemmas, perfect path, network security management obligations

1. Introduction

The demanding requirement of internet technology in cybercrime is causing criminals to commercially outsource the technology-related part of the crime. With the help of professional internet technicians, internet companies, criminals are able to do everything they want in cyberspace. In order to regulate this kind of neutral help behavior, China's Amendment IX to the Criminal Law stipulates the crime of refusing to perform the obligations of network security management. The object of regulation for this crime is network service providers, with the intention of eradicating

DOI: 10.54254/2753-7048/16/20231119

cybercrime from the top. However, since its stipulation, the crime has only been applied several times and has almost been reduced to a zombie crime [1]. According to statistics, as of April 16, 2023, only four cases have applied this crime. For this judicial application of the dilemma, there are the following explanations in the field of criminal law. The first issue is that the constitutive requirements are not clear, resulting in difficulties in judicial application [2]. The second issue is that the provision stipulates that one must be ordered to rectify and then refuse to do so, which actually sets too high of a threshold for incrimination. The regulatory authority's compositions and duties are also not clear, resulting in strict standards of conviction [3]. The third issue is that the crime's information network security management obligations are not clear. In judicial practice, there are questions about the necessities of setting this obligation [4].

In this paper, the authors take the case of Cheng Cong being entrusted by Chen Ming and others to manage the server and the case of Zhu Hao illegally selling VPN as examples to make an analysis. It can be found that the identification of the applicable subject, which is the network service provider, is not clear in this crime. At the same time, the obligation for network security management is also unclear. These two factors together lead to difficulties in ruling this crime. The network service provider's identification should be clarified firstly. Then, its management obligations can be concluded through the summary of its legislative intent. From another perspective, by comparing it with the crime of aiding network information crime, which has been reduced to a pocket crime in recent years, this paper argues that the similarities in the constituent requirements of the two crimes lead to a blurred boundary Between them. Judges tend to directly apply the crime of aiding information network crimes and ignore this crime. To solve this, this paper suggests that the boundaries Between the two crimes need to be further clarified in terms of the determination of knowing, the boundary Between consequential and behavioral offenses and the criminal patterns. Finally, based on the characteristics of the linkage mechanism Between administrative authorities and police, improvements should be made at the three levels of legislation, justice, supervision of law in order to alleviate the phenomenon of zombification and achieve the purpose of legislation.

2. The Dilemma of Application in Judicial Practice

2.1. The Ambiguity of the Identity of the Applicable Subject of the Crime

Since the definition of the internet service provider mentioned in the crime is complex, the judge may not have a comprehensive understanding of the crime and may overlook the specific status and regulatory obligations that come with it. As a result, the judge may directly apply the crime of aiding in network information crime. Cheng Cong, commissioned by Chen Hua, had been managing Chen Hua's servers operating LePan.com, which was confirmed as a site used to store and distribute pornographic films. Chen Cong provides technical services such as network connections, line repairs, domain name registration and server management. According to judicial interpretation, he should be considered a network service provider, which means he might commit the crime of refusing to perform the obligation of internet security management. However, the court completely disregarded this possibility. Moreover, during the server hosting, Cheng Cong's server was notified and administratively punished several times. Knowing this fact, he continued to host the server and did not rectify anything. Such behavior had fully met the constitutive requirements of this crime. However, the court directly applied the crime of aiding network information crime, which was thought to be a "pocket crime" among cybercrimes. The ignorance violates the principle of suiting punishment to the crime. As a result, not only can the purpose of legislation not be realized, but there is also a serious waste of judicial resources.

DOI: 10.54254/2753-7048/16/20231119

2.2. The Blurriness of the Boundary Between This Crime and the Crime of Aiding Network Information Crime

Due to the development of the black ash industry, criminals can arbitrarily combine the supply chain of crime according to the different nature of crime and enjoy the convenience of the supply of gray resources brought by the network [5]. That is the reason why the crime of aiding network information crime has already become a "pocket crime," in order to fundamentally eradicate cybercrimes on a wide scale. However, it has a lot in common with the crime of refusing to perform the obligation of internet security management, thus causing confusion. There are three aspects where authors thought boundaries are vague. The first point is knowing. While both of the crimes seem to potentially or explicitly require knowing, in fact, there are subtle differences in their composition. The other is the boundary Between behavioral and consequential offenses in the two crimes, and the last one is their criminal patterns. For example, Zhu Hao run several websites to promote the sale of his agents' VPN software for profit starting in 2016. In June 2017, Zhu Hao rented domestic and foreign servers to establish his own VPN platform and provided channels for others to sell online. In fact, VPN is a kind of criminal tool for illegal network intrusion. In terms of subjective objects, Zhu's VPN-related business promoted the sale of its agents' VPN software, providing users with tools that could be used for criminal activities. This is in line with the crime of aiding network information crime's constitutive requirements of "providing technical support or help to others to commit crimes". However, the court considered him a network service provider. Furthermore, since Zhu Hao was administratively punished by the authorities, he was convicted of this crime. At the same time, considering that the act of selling criminal tools itself is a crime, it does not require the users to produce criminal results. In other words, it is a consequential offense. It is not consistent with the nature of this crime, which involves a mixture of behavioral and consequential offenses.

3. Cause Analysis

3.1. The Identity of Network Service Provision

The first thing that needs to be clarified is the definition of network service provision. Further clarification is needed for the definition of internet service providers. Finally, it's necessary to clarify their obligations of being network service providers. The act of network service provision can be subdivided into three steps: hardware provision, local data management, and network access. Each of these steps is essential to achieve the ultimate goal, which is the normal operation of a website or software for regular user access. Therefore, the essence of the hosting work of the perpetrator in a large number of cases is to provide a sequence of auxiliary operational services in order to make the website available to users.

It should be mentioned, in particular, that such defendants do not have full control over the data they provide and the software they run. Therefore, it is impossible for them to know the source of all the data involved in the operation of the website. Meanwhile, it is impossible to require them to know all the details of the website. In other words, the crime of refusing to perform the obligation of internet security management in the application of judicial practice should not pay too much attention to the identify of whether the perpetrator knows the crime they have committed, but rather to the obligations themselves. At this point, his violation of provisions and the violation of two elements at the same time are key factors in the conviction of the internet service provider. Meanwhile, before the key to conviction, it can be seen from a large number of cases that the specific subject is the starting point for the beginning of conviction.

The crime of refusing to perform the obligation of internet security management is a typical form of negligence, as it involves neglecting one's responsibilities. Internet service providers have the

DOI: 10.54254/2753-7048/16/20231119

obligation to manage the personal information of citizens collected during the service process. If it has the ability to perform but fails to perform the statutory information network security management obligations, it should bear the corresponding inaction responsibility according to law [6]. Therefore, what specific obligations do internet service providers have? In terms of systemic interpretation, network security management obligations are prescribed by laws and administrative regulations. The law that comes first is the "Network Security Law" of the People's Republic of China, which was implemented in 2017. According to Article 47 of the Network Security Law, for the obligations of the server manager mentioned in previous cases, they should strengthen the management of the information published by the users. However, as mentioned above, the server administrator in most cases only has a certain amount of knowledge about the running data and does not have full control over it. Its obligation of supervision and management in this crime is limited, and the server administrator's omission should not be prosecuted too harshly. The scope of their obligations should be determined in relation to the scope of their service. Therefore, the legislator also regulates that "after the regulatory department orders corrective measures", the server provider also has an unlimited obligation to correct according to the instructions of the supervisory department to rectify. Therefore, the server administrator has a double obligation. The first point is the limited supervision and management obligation for the server, and the second is the unlimited correction obligation after receiving instructions from the regulatory department. Meanwhile, the administrative execution of regulatory authorities cannot be used alone as the only element of the crime. If the judgment of whether an act is criminal or not is based solely on the order of administrative authorities, the scope of punishment for the crime will be greatly reduced. This, in turn, will further affect the scope of application [7].

This particular category of management obligations for internet service providers is unique. As a result, upholding the principle "generalia specialibus non derogant", it should firstly be considered whether the defendant has breached such obligations in judgment. In judicial practice, the defendant may indeed meet the elements of the crime of aiding network information crime at the same time. However, in order to realize the principle of adaptation of crime and punishment, this behavior should be regulated by this crime.

3.2. The Boundary Between This Crime and the Crime of Aiding Network Information Crime

3.2.1. The Difference in Knowing

According to Article 286 of the Criminal Law, the subjective aspect of the judicial application of the crime of refusing to perform the obligation of internet security management is "being ordered by regulatory authorities to take corrective measures and refusing to comply," which indicates direct intention. Cheng Cong's defense opinion is completely contrary to the court's opinion. This suggests that the applicable standards for the application of "knowing" in judicial practice should be clarified. The definition of "knowing" is also one of the important factors to distinguish the two crimes. The establishment of the crime of aiding network information crime requires the perpetrator to know that others use the information network to commit crimes as a necessity. The perpetrator should clearly recognize the inevitability or possibility of harmful results occurring. If the perpetrator only has a vague understanding of the inevitability or possibility of the harmful result, even if the harmful result eventually occurs, it only proves that the perpetrator has indeed violated their duty of care. Further judgment is needed to clarify whether they can be held responsible for their negligence [8].

Therefore, during the conviction, the verdict of knowing should be analyzed in phases, including the defendant's direct intent for their own help behavior and the indulgence of the result of helping. For the aforementioned case of Cheng Cong, mandating the server in accordance with the contract is

DOI: 10.54254/2753-7048/16/20231119

a neutral help behavior, in line with the constitutive requirements of this crime. For Zhu, he held a hopeful attitude towards users who use VPNs to access the internet illegally. However, this behavior cannot be considered a neutral help behavior, which means the action is not applicable to this crime.

3.2.2. The Difference in Criminal Patterns

From the literal interpretation of the legal provisions, it can be seen that the perpetrator is an accessory criminal in the crime of aiding network information crime, while the crime of refusing to perform the obligation of internet security management is not the same. The former narrows the scope of the identity of the subject of the crime, while the latter can be both a principal and an accessory criminal in complicity. It can also be set up as a separate criminal individual, not constituting complicity. Among them, both the principal and accessory criminals can be identified only by the role they play in the complicity, while the establishment of a separate crime is less difficult to identify. In judicial practice, this difference in standards makes the latter easier to convict because whether the crime is principal, accessory, or separate, their effect on the verdict is slight. There is also no need to increase the difficulty for the judicial authorities to handle the case. In contrast, the conviction of the former is more difficult. First of all, complicity is very complex and the requirement of tracking the principal criminal in cyberspace undoubtedly increases its complexity. Secondly, in a specific network environment, identifying the perpetrator can also pose some difficulties. For example, the phenomenon of “an accomplice not necessarily being an accomplice”, “an accomplice not necessarily being an accessory”, “a principal not necessarily being a principal”, or “an accomplice without a principal” may exist.

In terms of criminal patterns, the standard for the crime of refusing to perform the obligation of internet security management makes it more applicable in judicial practice. This facilitates the lawful fulfillment of responsibilities by judicial authorities, which is conducive to improving the quality and credibility of judicial verdicts. It also enables criminals to take corresponding criminal responsibility and allows the innocent to be cleared of crimes. Meanwhile, it is also conducive to preventing the crime of aiding information crimes from becoming pocket crimes.

3.2.3. The Boundaries Between Consequential Offence and Behavioral Offence

According to Article 286 of the Criminal Law, the objective aspect of the crime of refusing to perform the obligation of internet security management is that “the internet service provider does not perform the obligations of information network security management regulated by laws and administrative regulations”, and “the supervisory department orders corrective measures and the provider refuses to comply.” This paper argues the premise of the regulatory department ordering correction is the perpetrator’s illegal practice, which has already resulted in the infringement of legal interests. Therefore, the difference Between its objective aspect and the crime of aiding network information crime is also traceable. The latter’s objective aspect will focus more on helping behavior. Thus, whether the helping behavior causes infringement of legal interests or not, the objective existence is implemented to satisfy the elements of the crime. The act of authorizing, aiding, or assisting is not criminal. Its criminality stems from the behavior itself, rather than the object of these behaviors [9]. At this point, the latter crime lowered the cybercrime threshold, making it probably a “pocket crime”. While the threshold for the former crime is slightly higher, its standards in the objective aspects lead to the former’s applicability in judicial practice, resulting in a more specialized scope of conviction. It is one of the main reasons for its low frequency of use.

DOI: 10.54254/2753-7048/16/20231119

4. Optimized Path

The network environment provides an "invisible" place to accommodate multiple services. Its concealment and polymorphism make it complicated and difficult for investigative authorities to track criminal acts. In addition, the lack of popularization of network-related laws and regulations in various regions has led to many cases involving the crime of refusing to fulfill the obligation of information network security management in recent years. In terms of its role, cybercrime often facilitates criminal behavior by breaking through technical obstacles, allowing ordinary people who lack the ability to commit cybercrime to participate. Meanwhile, network technology support usually plays a decisive role in the realization of cybercrime [10]. With the intervention of information networks, the division of labor in cybercrime has become the norm, leading to obvious variations in the elements and patterns of crime. It can be said that cybercrime, under the division of labor, is by no means a simple replica of traditional crime in cyberspace, but presents a new criminal pattern [11]. If the traditional concept of criminal law is still used to interpret cybercrime today, the punishment mode in judicial practice can only skirt around the issue instead of effectively and truly solving the problem.

4.1. Responsibilities of the Legislature

The author believes that the legislative purpose of the crime of refusing to fulfill the obligation of information network security management in Article 286 has the following points. Firstly, China should improve laws and regulations, enhance the Chinese rule of law system, and update the "Criminal Law" to keep up with the times. Secondly, China should make "criminal law" the foundation of the legal system and define the minimum requirements for more specialized laws and regulations, such as the "network security law," to reduce the frequency of crimes committed by industry personnel. Thirdly, China should cut off more downstream cybercrime, eradicate the vertical and horizontal extension of the industrial chain of cybercrime and deter network service providers from weakening network security through punishment to curb criminal acts that undermine network security [12].

Based on the above purpose, this paper can propose corresponding improvement measures. For the legislature, it should keep pace with the times by promulgating specific judicial interpretation opinions, updating guiding cases, and facilitating the accurate judgment of judicial authorities. At the same time, relevant articles should be added to the amendment to further standardize the legislative system and provide subordinate authorities with a legal basis to follow. This will better reference the unified standard applicable to judicial practice.

4.2. Responsibilities of the Judiciary

Whether the crime of refusing to perform the obligation of information network security management will be further reduced to a "zombie crime" is related to every judicial authority's handling of the case. The change in attitude of judicial authorities, from an active approach to a more prudent and accurate attitude, is aimed at preventing oversimplification of convictions that may lead to wrongful convictions and violations of criminal justice. This transformation can also help prevent the crime of aiding network crimes from falling into more and more dilemmas [13].

The author believes that the judicial authorities should make improvements in the following aspects. Before accepting cases, the administrative authorities should reduce the negative pressure of the case registration system of the judicial authorities and particularly pay attention to procedural justice. In the process of a trial, judges should reasonably exercise their discretion based on a thorough study of the original law article and judicial interpretation. They should formulate unified discretion standards and minimize the occurrence of case variables. In the process of sentencing, Chinese

DOI: 10.54254/2753-7048/16/20231119

judicial authorities should strictly adhere to the requirements of the law and its corresponding punishment articles. In view of the complex situation of "serious circumstances", Chinese judicial authorities must also abide by the principle of legality and make reasonable sentencing in combination with the judicial interpretation and guiding cases promulgated by the legislature and the actual judicial situation. China's judicial authorities should carefully consider whether the perpetrator has the subject qualification of a network service provider, screen their criminal intent and implementation, and pay reasonable attention to avoiding all potential criminal risks. This will ensure that offenders cannot use safe harbor rules as a shield to evade criminal penalties.

Due to the breakthrough of the network environment for regional space, the jurisdictional application involved in cybercrime tends to be complicated. As an important part of the network environment governance chain, the procuratorial authorities have the right and obligation to bear responsibility for the current practice dilemma of the crime of refusing to fulfill the obligation of information network security management. In handling related cases, courts should coordinate and implement a cross-regional case-handling mechanism, integrate case-handling forces, and form a joint force [14]. The procuratorial authorities supervise the administrative supervision departments downwards, assist in law enforcement review work, track illegal cases, and jointly govern cyberspace.

4.3. Responsibilities of the Regulatory Authorities

The right of supervision is the cornerstone for the proper performance of judicial power. As the first step in the condemnation process, regulatory authorities have the right to perform their duties based on legal provisions and judicial interpretations of this crime. They should also carry out administrative law enforcement in accordance with relevant provisions on time. It is the primary executor of the conviction and sentencing of this crime in the specific practice of judicial application. Therefore, regulatory authorities are also obliged to supervise and manage network service providers and promptly issue corrective orders to increase crackdown on illegal personnel. The correction of orders by the supervisory department is one of the important links in the chain of the perpetrator's crime. Only when the supervisory department issues correction orders for the suspected perpetrator can the objective aspect of the crime be satisfied. Therefore, law enforcement agencies and the judiciary should coordinate their relationship, mutually assist each other, and forbid interference with the function and responsibility of the other authority. The regulatory authorities should also take this crime patterns as a practice rule, standardize the supervision and review system, clarify the difference Between industry norms and criminal laws and regulations, and carry out measured order.

In addition, attention should be paid to the determination that "the regulatory authorities ordered corrective measures and refused to comply." The necessary judicial review should be carried out on the corrective action ordered by the regulatory authorities, and the legality and rationality of the ordered behavior should be examined thoroughly. In addition, it is necessary to consider whether the current technical level has the ability to identify other perpetrators and punish them [14]. Therefore, the regulatory authorities also need to improve their ability and quality of supervision and management, and timely perform their duties of supervision, control, and handling illegal network service behaviors. Local regulatory authorities should also improve their mastery of network technology. Especially, the administrative authorities should take initiative to ensure that the objective elements of this crime are not absent.

5. Conclusion

This paper focuses on the dilemma of judicial application of the crime of refusing to perform the network security management obligations. For the problem of unclear applicable objects and vague boundaries Between this crime and the crime of aiding network information crimes, this paper

DOI: 10.54254/2753-7048/16/20231119

proposes specific identification standards to assist judges in better applying this crime. As for the underlying cause behind these problems, this paper suggests the respective improvements from three perspectives including legislation, justice and supervision. For legislation, the legislature should legislate for the characteristics of cybercrime to keep up with the times. For the judiciary, courts and prosecutors, it is not appropriate to apply pocket crimes for the sake of convenience. They should combine the judicial interpretations and guiding cases promulgated by the legislature with the actual judicial situation to make a reasonable conviction and sentence in the judgment. For the supervisory department, due to the characteristics of the linkage Between the execution and punishment of this crime, the supervisory department should make every effort to fulfill its supervisory duty and issue corrective instructions in a timely manner. In the face of the new situation of cybercrime, new methods should be adopted. That is the reason why this crime is established for this purpose. Although there are still many problems with this crime, this paper hopes that the research in this paper can inspire the amendment of relevant laws. the vigilance of regulatory authorities for cybercrime and the accuracy of law enforcement should be improved. This will reduce the perception of miscarriage of justice and promote judicial fairness. However, the crime of refusing to fulfill the obligations of network security management is still unclear in terms of the allocation of regulatory obligations. Although the mainstream belief worldwide is that network service providers do not have any regulatory obligations, this is inconsistent with China's national conditions. The specific allocation of responsibilities Between network service providers and regulatory authorities is still subject to study and discussion.

References

[1] *Chen. H.B. (2022) Reflection on the "Zombification" of the Crime of Refusing to Fulfill the Obligation of Information Network Security Management. Academic Forum,3:1-12.*

[2] *Chen. H.B. (2022) Examining the legislation and application of China's new information network crime. Journal of Guangxi University (Philosophy and Social Science),2:185-198.*

[3] *Wang. S. (2022) An Interpretation on "Ordering to Take Corrective Measures" in the Crime of Refusing to Perform the Information Network Security Management Obligation: Thoughts on Interconnection of Administrative and Criminal Regulations. Journal of Law Application,8:75-84.*

[4] *Shanghai Putuo District People 's Procuratorate Research Group, Zhu. W.B. (2021) A Research on the Criminal Liability of Internet Service Providers. Criminal Research,6:93-100.*

[5] *Chen. X.B., Wang. X.C. (2021) Complicity Imputation Dilemma and Theoretical Reconstruction of Cyber Technical Service Complicity Type. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition),35(1):67-79.*

[6] *Li. M.L. (2022) Research on the Responsibility of Network Service Providers' Omissions in the Crime of Telecommunication Network Fraud. Journal of Information Security Research,8(2):165-171.*

[7] *Li. B.C. (2017) Two - sidedness of the Crime Refusing to Fulfill the Information and Network Security Management Obligation. Legal Forum,32(3):138-145.*

[8] *Huang. Z.J., Zhang. Z.Y. (2021) Regulation Analysis and Judicial Application on the Crime of Helping the Information Network Criminal Activity. People's Procuratorial Semimonthly,23:49-53.*

[9] *Chen. X.L. (2022) Turning the Accomplice into the Perpetrator: Perspective from the Crime of Providing Assistance in Cybercriminal Activities. Journal of Comparative Law,2:44-58.*

[10] *Zhang. W. (2023) The Dogmatic Study of the Crimes of Providing Assistance in the Web-Based Criminal Activities. Journal of Comparative Law,1:97-111.*

[11] *Yu. H.S. (2022) Fragmentation of Cyber Crime and Systematization of Criminal Governance. Science of Law (Journal of Northwest University of Political Science and Law),3:58-70.*

[12] *Mai. X.L. (2021) The Correction of the Dislocation Between Network Security Management Obligation and Criminal Obligation: From the Perspective of the Crime of Refusing to Fulfil the Network Security Management Obligation. Journal of Ankang University,33(2):106-111.*

[13] *Mao. B. (2022) Reflection on the dilemma in determining the knowledge element of the aiding cybercrime offense. Evidence Science,30(6):730-742.*

[14] *Ma. C.Y., Ren. P.B. (2020) The crime of refusing to fulfill the obligation of information network security management: practical dilemma, legal connotation and countermeasure. The Theory and Practice of Improving the*

DOI: 10.54254/2753-7048/16/20231119

Governance of Cybercrime in Criminal Procuratorial: The 16th National Senior Prosecutor Forum. 505-511.10.26914/c.cnkihy.2020.047378.