Law and Humanities
ISSN Print: 3079-5117
ISSN Online: 3079-5125
https://doi.org/10.63313/LH.9022

Research on the Crime of Helping Information Network Crime

Yu Zhou
Anhui University of Finance and Economics, Bengbu 233030, China
Email: 3481557495@qq.com

How to cite this paper: Zhou, Y. (2025). Research on the Crime of Helping Information Network Crime. Law and Humanities, 1(3), 22-30. ISSN Print: 3079-5117; ISSN Online: 3079-5125.
https://doi.org/10.63313/LH.9022
Published: 2025-07-07

Abstract

As cybercrime methods become increasingly hidden and unpreventable, it is difficult to effectively curb the development of new cybercriminals through the use of traditional crimes. From the perspective of criminal law provisions, helping information-networked crimes is a new type of crime. However, in judicial practice, confusion was caused by the generality of the legal provisions of the applicable rules for this offence, resulting in different sentences for the same case for this offence. Therefore, this paper looks at several difficult issues in determining this crime in depth, in order to provide certain references to judicial practice.

Keywords

Crime of aiding information network criminal activities; The constitution of the crime; Serious circumstances; Joint crime

Introduction

The development of information networks has made people's lives more convenient, but it has also increased the risk of potential infringements. Therefore, the law must respond quickly and effectively to protect against these risks. In the absence of information network crimes, many criminals exploit the delays in the legal system to seek illegal gains. In this context, the crime of aiding information network crimes (hereinafter referred to as' aiding information crimes ') emerged and was included in the Criminal Law Amendment (IX) enacted in November 2015. The establishment of this crime is crucial for combating information network crimes, protecting citizens' property, and maintaining network order. However, due to its late establishment and numerous challenges in judicial practice, the application of the law remains problematic, with many defects and controversies in reality. This article provides a basic analysis of the subject and object of this crime, summarizes real-life issues, and proposes feasible methods from a legislative perspective.

1. The legislative background of the crime of assisting information network criminal activities

In the Internet age, the data-centric Internet has significantly increased the frequency of information exchange in the real world. The deep integration of the Internet with traditional industries has intensified, but new forms of cybercrime, such as telecom fraud and spam messages, have also become more prevalent. To address these rapidly evolving issues, China's Criminal Law should adapt to the times by strengthening legislation and using state power to combat the growing cybercrime. For instance, the Criminal Law Amendment (IX) includes four specific provisions targeting cybercrime, with the most notable feature being the establishment of aiding and abetting cybercrime as a separate offense.

2. The legislative problems existing in the crime of assisting information network crimes

2.1. The scope of the penalty standard is too broad

The crime of aiding and abetting is categorized as an activity that infringes upon and hinders social management order within the broader context of criminal law. For this type of crime, the object of the offense is social order, which in the digital realm translates to network order. Therefore, if the act of assistance disrupts the social order within the network, it constitutes this crime. This crime was established to fundamentally combat the acts that facilitate cybercrime, thereby severing the entire criminal chain. Generally, if an act must be punished by criminal law after evaluation, it must have objectively harmed legal interests. The establishment of this crime is due to the increasing prevalence of internet crimes, which pose significant threats to internet security and the personal and property safety of citizens. However, the legislative body did not consider all aspects comprehensively when establishing this crime, leading to the inclusion of many acts within its scope of punishment, making the standards for punishment very lenient. In the crime of aiding and abetting, the scope of punishment is extremely broad, resulting in numerous 'wrong cases.' These cases highlight issues such as the blurred line between 'aiding behavior' and 'neutral aiding behavior,' the ambiguous definition of 'knowingly,' and overly broad subject determination.

2.2. Unclear criteria for identifying accomplices

The traditional accomplice theory adopts the subordinate theory, which posits that an accomplice's actions must be subordinate to and dependent on the principal offender. According to this theory, a joint crime is established if: first, there are at least two subjects, which can be either entities or individuals; second, a common intent is a necessary subjective element of a joint crime, requiring mutual interest, shared understanding, and a common will; third, objectively, each participant must engage in a joint action. Only when all three conditions are met can an accomplice and the principal offender be considered as a joint crime.

2.3. The boundary with other crimes is unclear

2.3.1. With fraud

Cyber fraud is a common form of criminal activity that exploits information networks. In the context of fraud, the act of committing fraud is considered the primary crime, and any assistance in this process can also be seen as part of the fraud. However, aiding in a crime does not require deception but rather assistance. In the case of Li Mou for aiding in information crimes, he was convicted and sentenced for this offense. In the case of Wang Mou for fraud, he was identified as a suspect due to fraudulent activities. Case studies show that the criminal acts of these two individuals are very similar. Objectively, both engaged in assisting others in committing fraud. However, their legal evaluations and punishments differ significantly. The relationship between these acts is crucial for determining and punishing them. However, from the current legal framework, it seems difficult to clearly distinguish between them through textual interpretation.

2.3.2. Money laundering

The Criminal Law of our country has relatively comprehensive provisions for punishing money laundering crimes. However, the scope of punishment for this crime is closely related to that of aiding and abetting crimes. The nature of these two crimes is very similar, and they share many similarities in their outward manifestations. For example, assisting upstream crimes by providing bank cards and other payment settlement services may be considered both aiding and abetting crimes and money laundering crimes. Both crimes require that the perpetrator's subjective intent be intentional and related to the upstream crime. Therefore, in practical matters, accurately recognizing these two crimes is crucial.

3. Understanding the constitutive elements of the crime of assisting information network criminal activities

3.1. Understanding of the object of the crime

The object of this crime should be the order of information network management. Firstly, from its position in China's Criminal Law, this crime is categorized as a crime that disrupts social management order. Moreover, the order of information network management is a crucial component of social management order. Therefore, the legislative intent behind placing this crime in this category is to confirm that the order of information network management is the object of this crime. Secondly, China's Criminal Law defines the establishment of assisted criminal acts, which infringe upon indirect and diverse legal interests. However, in criminal law, the object of a separately established crime must be relatively clear. If different acts infringing upon various legal interests are determined separately, it would contradict the legislative intent. Therefore, using 'public places' as the network space as the object of the

crime, and on this basis, taking this as the object of the crime, better aligns with China's legislative intent. Thus, the object of this crime should be the order of information network management.

3.2. Understanding of the objective aspect of the crime

3.2.1. Understanding of helping behavior

According to the relevant provisions of the Criminal Law on this crime, we can know that for this crime, its harmful behavior is very complicated, its types are also various, but its specific behavior mode mainly has the following two:

3.2.2. Judgment of serious circumstances

Serious circumstances are a necessary element for constituting this crime, but this also limits the penalizability of the crime. While a general description of the crime is more adaptable to development, the lack of clear regulations has led to a very vague scope of punishment, lacking a specific and operational standard, which violates the principle of clarity in criminal law. In 2019, the Supreme People's Court and the Supreme People's Procuratorate issued an interpretation regarding the crime of aiding and abetting due to its overly vague application in practice. Article 12 of this interpretation clearly defines the specific standards for 'serious circumstances,' detailing seven specific scenarios. This not only highlights the harmfulness of the assisting behavior but also reflects the perpetrator's subjective malice and potential harmful consequences.

3.3. Understanding of the subject of the crime

3.3.1. Scope of the subject

The perpetrator of this crime should be a general subject, but it is also important to note that Internet service providers are a relatively special category. According to the provisions, Internet access service providers, payment and settlement platforms, and other network service providers are the primary subjects of this crime. However, with the rapid advancement of technology, the perpetrators are no longer limited to technical personnel; anyone can commit this crime, thus broadening the scope of the perpetrator.

3.3.2. Definition of crimes committed by natural persons

Natural persons are the subjects of this crime and are the primary perpetrators. According to legal provisions, anyone who provides assistance in cybercrime is considered an accomplice, thus meeting the objective criteria for being a subject. However, normal business activities of natural persons should not be considered crimes. For instance, in the case of Leng Moumou's assistance in information-related crimes, Leng Moumou rented a landline in his registered Taobao store. The court ruled that

the defendant knew that the phone user would use the phone for illegal activities but still provided telephone forwarding and other communication services, resulting in the victim Lou Mou being defrauded of 3.59 million yuan. Therefore, it should be determined that his act of renting a fixed telephone number constitutes the crime of assisting fraud. In the author's view, renting a fixed number is a legitimate business activity, similar to when someone uses the telephone services of the three major telecommunications companies for fraud, relevant units cannot be charged with aiding information-related crimes.

3.4. Understanding of the subjective aspect of this crime

3.4.1. The form of culpability of this crime

The Criminal Law provides a detailed description of "knowingly allowing others to commit crimes through information networks." As part of the legal provisions, this is also a subjective condition that must be met by those who assist in such acts. Therefore, whether this crime is established depends on whether the perpetrator has the intention to assist. In criminal law, subjective intent is interpreted as either hoping or allowing, which is also a factor of will. Generally, when determining criminal intent, we consider two aspects: "knowingly" and "hoping or allowing," both of which must be present for it to be determined that the perpetrator has the intention to assist.

3.4.2. Definition of "knowing"

The legislative provisions do not clearly define 'knowingly,' and there is no unified view in the academic community. Different interpretations include: 'knowingly' refers to 'indeed knowing,' meaning a clear awareness. Some argue that 'knowingly' originally meant clear knowledge or understanding, which means: 'the perpetrator has long known or should have known about a certain fact or its possibility, but this does not include being presumed to know.' 'knowingly' encompasses both 'indeed knowing' and 'should have known.' The academic debate centers on the scope of 'should have known.' Some propose that only when the scope of 'should have known' is sufficiently broad can it be considered 'knowingly.' Professor Liu Xianquan introduced the 'over half principle' in the Criminal Law, suggesting that if evidence shows that the criminal act constitutes more than 50% of all criminal acts, it can be presumed that 'should have known.' 3) 'knowingly' includes both 'indeed knowing' and 'possible knowing.' Professor Li Hong argues that 'knowingly' should encompass both 'indeed knowing' and 'possible knowing,' and 'possible knowing' must be determined based on the specifics of the case. For example, if the identity information and other relevant information used by users when enjoying your services are false, and you knew or should have known about this, it can be concluded that you had the possibility of knowing.

4. Improving the legislation of aiding information network crimes

4.1. Clarifying the scope of punishment for aiding information network crimes

4.1.1. Limit the scope of subjects

The academic community holds that network service providers are the core of network information transmission and the primary actors in this crime. However, after reviewing relevant cases, the author believes that in judicial practice, individuals are the main actors. The characteristics of assistance in cybercrime include: In practice, the perpetrators are often individuals with specific information network technology skills, while network service providers are a minority. Individuals who provide such assistance typically do not belong to any network platform or company but can offer network products and related services at the request of others. In real-world criminal cases, assistance provided by individuals with professional network skills often involves being invited to help or transitioning their main business to providing network services, thereby contributing to cybercrime. Therefore, those who assist will provide assistance according to the client's requirements and ideas, so in a sense, those who assist in cybercrime must have some understanding or knowledge of the crime before joining the criminal activities and performing the relevant assistance.

4.1.2. Refine the subjective "knowing"

The subjective aspect of this crime is intentional, which includes both the cognitive element of 'knowing' and the volitional elements of hope or indifference. This means knowing that helping would lead to danger but still harboring an expectant or indifferent attitude. The 'knowing' in this crime should encompass both 'indeed knowing' and 'should know.' Given that this crime targets new types of cybercrime characterized by 'one-to-many' and 'cross-regional' features, and there is no meaningful connection between the helper and the assisted, proving the helper's subjective awareness is challenging. If' knowing 'only includes' indeed knowing, 'forming a complete chain of evidence would be extremely difficult, significantly reducing the operability of this crime and making it impossible to achieve the target of crackdown. If a broader standard is adopted, where' knowing 'includes both' indeed knowing 'and' possible knowing, 'the' crackdown 'under this standard would be too broad, leading to a serious disconnect with the helper's own subjective psychology. This not only fails to protect their legitimate rights and interests but also hinders the development of the Internet information age.

4.2. Determine the criteria for identifying accomplices in the crime of identification

If we study from the perspective of joint crimes, an accomplice should be a form of joint crime. Fundamentally, an accomplice in a joint crime is not the one who plays a decisive role. Moreover, without the presence of the principal offender, the concept of an accomplice does not apply. The relationship between the aiding act and the principal act is one of subordination, where one is subordinate to the other. Therefore, to define an accomplice, the existence of the principal offender must be a prerequisite; the term 'aiding' must also have some social harmfulness. Otherwise, all Internet technical services related to the act could be considered 'aiding' (for example, using a new base station created by a service provider for fraud when there is no social harmfulness). If someone helps without criminal intent, controls their own behavior, and significantly influences it, they should be recognized as the principal offender.

4.3. Make clear the boundary between the crime of assisting information network crimes and other crimes

4.3.1. The boundary with the crime of fraud

From a subjective standpoint, when helpers provide information to others, they do not necessarily have the criminal intent of fraud. However, they merely offer online services for others' criminal activities without being aware of the actual fraudulent acts. When discussing accomplices in fraud, it is necessary that the accomplice has a conspiracy in mind and that this is evident when they assist or incite others. This means that the accomplice also has the intention to gain financial benefits. However, at this point, the helper clearly lacks or may not possess such a subjective intent. The helper primarily aims to earn labor compensation from those who commit specific crimes through these services, rather than defrauding money from the victims.Objectively speaking, in certain criminal activities, the information network is used to help the perpetrator provide Internet access and other services. On the surface, it is easy for the judge to determine that the accomplice and the fraudster are conspirators, but in fact, the accomplice is only a duty act, not a duty act.To sum up, when the crime of aiding information and the crime of fraud appear to be imagined competition, the crime of aiding information should be taken as the final judgment result and sentenced for the crime.

4.3.2. The boundary with concealing guilt

The provisions for the crime of concealing and covering up are outlined in Article 312 of the Criminal Law, both aimed at maintaining the order of information network security. However, the crime of concealing and covering up and the crime of concealment are two distinct offenses, each describing different scenarios. In the crime of concealing and covering up, the offense is primarily premised on the completion of the upstream crime, which is a crime involving illicit gains. While the crime of concealing and covering up shares some similarities with the crime of con-

cealment, there are significant differences in certain aspects, specifically as follows:

Epilogue

The rapid development of the Internet and the continuous innovation in information technology have made network technology a significant force for social progress. However, this has also led to an increase and intensification of cybercrime. Criminal law is a set of rules that are essential for maintaining market and social order. In terms of legislation and legal theory, it is crucial to promptly address the issues arising from cybercrime. In this process, legislators have recognized that many individuals engage in a range of criminal activities through information networks. As a result, the crime of aiding and abetting information network crimes has been established as a separate offense, providing a legal basis for regulating information network activities.

This article begins by analyzing the issues present in the legislation of this crime. It then delves into the relevant issues from the perspective of the elements constituting this crime, offering solutions to these problems. Regarding the objective aspects of this crime, it addresses two main areas: first, the object of the crime, and second, the acts of assistance, specifically providing technical support for cybercrime and offering advertising and payment settlement services for cybercrime. These two types of acts are common in the criminal activities related to this crime. Additionally, the article lists the criteria for determining serious circumstances based on the legal provisions of this crime.

Regarding the subjects and subjective aspects of this crime, it first outlines the scope of the subjects, concluding that the subjects of this crime are not limited to technical workers but also include individuals who provide various forms of information technology or network assistance to others. The understanding of the subjective aspect of this crime is approached from several angles: first, the form of culpability. Unlike the definition of 'knowingly,' which is not clearly defined in the legislative provisions, there is no consensus on this issue in theory. Finally, the article begins by improving the legislation for the crime of aiding and abetting, categorizing it into three types, analyzing the scope of the crime's applicability, the criteria for identifying accomplices, and the boundaries with other crimes, and proposes improvements in these three areas.

References

[1] Sun Yu. On the Protection Rules for Internet Service Providers —— From the Perspective of Limitations on Criminal Liability [M]. Beijing: China Legal Publishing House, 2019,45-56.

[2] Criminal Law (Volume I: General Theory) [M]. Beijing: Higher Education Press, 2019,111-123.

[3] Wang Aili. Interpretation and Application of the Criminal Law of the People's Republic of China [M]. Beijing: People's Court Press, 2021,564-569.

[4] Chen Xingliang. Criminal Law Value Construction Theory [M]. Beijing: China Renmin University Press, 2006,49-70.

[5] Zhang Mingkai. Criminal Law [M]. Beijing: Law Press, 2021,256-268.

[6] Zhao Bingzhi. Interpretation and Application of the Criminal Law Amendment (IX) of the People's Republic of China [M]. Beijing: China Legal Publishing House, 2016,33-48.

[7] Zhou Guangquan. Criminal Liability Scope of Internet Service Providers [J]. China Law Review, 2015, (2),14-16.

[8] Liu Xianquan. Criminal Responsibility for the Abuse of Information Network Technology [J]. Political and Legal Forum, 2015, (6),2-5.

[9] Liang Genlin. Traditional Crime Networking: Attribution Obstacles, Criminal Law Response, and Doctrinal Restriction [J]. Law, 2017, (2),9-15.

[10] Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Network and Assistance in Information Network Crime [N]. Procuratorial Daily, 2019-10-27,6-7.

[11] China Internet Network Information Center.37 Statistical Reports on the Development of China's Internet [R]. 2016,56-60.

[12] Provisions of the People's Procuratorate on Handling Internet Crime Cases [S]. China National Radio Network, 2021,33-40.