Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/57/20240094

The Identification of "Knowingly" in Crime of Assisting in Information Network-Related Criminal Activities

Zhihan Liu[1,a,*]

[1]*School of Humanities and Law, Hebei Normal University of Science &Technology, Qinhuangdao, China*
a. liuzhihan@ldy.edu.rs
**corresponding author*

Abstract: In recent years, with the rapid development of network technology, the frequency of cyber crime cases has been increasing, and the criminal means are emerging in an endless stream. The Criminal Law of the People's Republic of China (IX), introduced in 2015, added crime of assisting in information network-related criminal activities. Once this crime has been introduced, there are many discussions on the definition of "knowingly", which may lead to the application of this crime too extended or limited. In order to solve this problem and better understand and apply the law, this paper mainly uses three research methods: literature research, case analysis and comparative analysis. Firstly, in terms of understanding the connotation of knowing, "knowing" is understood as "clearly knowing" and "should know". Secondly, the object of "knowing" is clearly defined. Understanding "knowingly" objects as "criminal acts" that conform to the objective aspects of specific criminal acts is sufficient. Finally, a method for identifying "knowing" is proposed, with a focus on adhering to the principle of combining subjectivity and objectivity.

Keywords: Crime of assisting in information network-related criminal activities, Knowingly, Should know, illation, crime

1. Introduction

In recent years, with the development of science and technology, the types of communication technology have increased, and information network technology is inseparable from people's lives, providing a hotbed for related crimes. The number and frequency of "two-card" crimes in telecom fraud are increasing year by year. In order to crack down on the "two cards" criminal activities, maintain the information network environment, and protect the safety of people's property, the Ministry of Public Security launched the "Card Breaking Operation" nationwide on October 10, 2020. The 36th Session of the Standing Committee of the 13th National People's Congress passed the Anti-Telecommunications Network Fraud Law, which further reflects the importance that the state attaches to information network security, as well as the necessity and urgency of dealing with related crimes.

At the beginning of the legislation, the number of crimes committed was not high, but since the Supreme People's Court and the Supreme People's Procuratorate issued the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases such as Illegal Use of Information Networks and Aiding Criminal Activities on Information Networks in 2019, the number of cases related to the crime of aiding and trusting has increased rapidly. In addition, due to the

DOI: 10.54254/2753-7048/57/20240094

characteristics of network technology, some crimes are closely connected with upstream and downstream crimes, presenting a complete criminal industry chain [1]. This phenomenon reflects that one of the problems existing in the crime of aiding and abetting trust is the difficulty in determining "knowingly". The subjective aspect of crime of assisting in information network-related criminal activities is the state of mind that one's act of providing assistance to others in the information network crime will cause damage to the state's information network management order, and still hopes that it will occur. However, the law does not specify the degree of "knowing". As a result, it is difficult to grasp the degree of knowledge in judicial practice, and the problem of different judgments in the same case may arise. Therefore, in order to solve the determination of "knowingly", it is necessary to clarify the basic meaning of "knowingly"; the object of "knowingly"; The standard for determining "knowingly".

2. The Practical Dilemma of Determining "Knowingly" in Crime of Assisting in Information Network-Related Criminal Activities

2.1. Differences in Understanding the Meaning of "Knowingly"

The law does not have specific provisions or uniform standards for the connotation of "knowingly". In judicial practice, there are cases where judges make judgments based on their own understanding of "knowingly". Similar cases will have different verdicts under different judges' decisions. This is not conducive to the fairness of the judgment.

There are also many different views on the degree of "knowing" in the academic community. The first view is that "knowingly" simply means "knowingly". The second view is that "knowingly" should include "expressly knowing" and "ought to have known". A third view is that "knowingly" includes "actually knowing" and "probably knowing". In judicial practice, there are three kinds of mixed views.

2.2. Different Views on "Knowing" Objects

The concept of crime of assisting in information network-related criminal activities is "the act of clearly knowing that others are using information networks to commit crimes, providing them with technical support such as Internet access, server hosting, network storage, and communication transmission, or providing assistance such as advertising and promotion, payment and settlement, where the circumstances are serious." It can be seen from this that the object of the crime of aiding and believing refers to the downstream "criminal act" that is aided by the act of aiding and believing. Interpreting the concept of "criminal conduct" plays an important role in correctly determining the subjective "knowledge" of a criminal suspect in crime of assisting in information network-related criminal activities.

There are three main views on what is "knowing". The first view is that the "crime" must be a criminal act that meets the elements of the crime. The second view was that it was sufficient to understand "crime" as "ordinary offence". The third view is that "crime" is an illegal act that corresponds to the objective aspect of a specific crime [2].

2.3. Differences in the Criteria for Determining the Subjective Aspect of What Constitutes "Knowingly"

There is a lack of clear norms for determining the standard of knowledge in crime of assisting in information network-related criminal activities, and in judicial practice, there is a problem of relying too much on the evidence of confessions to find out the subjective "knowing" situation. And in the process of handling real cases, the suspect has a fluke mentality. In order to escape the law, they

DOI: 10.54254/2753-7048/57/20240094

usually insist that they do not know anything in the process of making confessions. This will put pressure on the investigation and evidence collection, and the accuracy of the evidence can only be confirmed by repeatedly making confessions to the criminal suspect, so as to ensure the accuracy of the evidence. At the same time, in the course of the trial, there will also be resistance to the progress of the trial due to insufficient evidence. or because of excessive reliance on confessions, the true intentions of the criminal suspect cannot be known, and in serious cases, unjust, false and wrongly decided cases arise. This would allow those who did not have the necessity of punishment or acts of neutral assistance to be wrongly convicted, and those who should have been convicted would escape the punishment of the law. Neutral helping behavior here includes "neutral business behavior", which is a concept first proposed in Germany. Neutrality means that regardless of whether or not the person who is helping the business has committed a criminal act, the business person will carry out normal business activities in accordance with the requirements of the profession [3].

3. Assist in the Understanding and Analysis of "Knowingly" in Crime of Assisting in Information Network-Related Criminal Activities

3.1. Three Views on the Basic Meaning of "Knowingly" and Their Differentiation

Article 287-2 of the Criminal Law of the People's Republic of China provides: Clearly knowing that others are using information networks to commit crimes, providing them with technical support such as internet access, server hosting, network storage, and communication transmission, or providing assistance such as advertising and promotion, payment and settlement, etc. There are three main views on the meaning of "knowingly".

The first view is that "knowingly" means "clearly knowing", that is, the perpetrator clearly knows that another person has committed a criminal activity and provides assistance to him [4]. This view rejects the expansion of the meaning of "knowingly", arguing that the expansion of the meaning of "knowingly" would lead to the blurring of the definitions of the two concepts of "willfulness" and "negligence" in the crime.

The second view is that "knowingly" includes both "knowing with certainty" and "probably knowing" [5]. The so-called "possible knowledge" means that the perpetrator has a suspicious attitude towards the criminal acts of others, and it is a state of possible knowledge. This view is based on the difficulty of determining that the subjective aspect is "clearly known" in judicial practice. The mere identification of this situation as a subjective aspect of the offence may lead to indulgence in criminal behaviour. Therefore, it is necessary to expand the scope of the meaning of "knowingly" to a certain extent. In the case of Zhang's assistance in information network criminal activities. The court held that the defendant Zhang Moumou clearly knew that he sold the bank card to others, and that others might use the bank card to commit criminal acts, but still provided payment and settlement assistance to him. Zhang's actions have constituted crime of assisting in information network-related criminal activities [6]. The case falls under the category of "probably known". It is important to note that "may know" and "know maybe" are two completely different meanings.

The third view is that "knowingly" should include two states: "clearly knowing" and "ought to have known" [7]. The so-called "ought to know" is presumed to know. Where the perpetrator provided the aid, it can be presumed that he was aware of the criminal act of the person being helped, and it is difficult to say that the perpetrator was unaware of this fact. In the case of Guo Moumou's assistance to information network criminal activities, the court held that Guo Moumou sold two sets of bank cards he handled to Tao, a stranger who knew that there were many local telecommunications frauds, in order to make a profit. Guo Moumou's own confession also said that he knew at that time that Tao Moumou and others might use bank cards to do illegal things. After Guo Moumou returned to his hometown, he was worried about the problem with the bank card, so he went to the bank to check

DOI: 10.54254/2753-7048/57/20240094

and cancel it. From the above acts, it can be inferred that Guo Moumou should have known that Tao Moumou would carry out criminal activities [8].

In general, it is better to adopt a combination of "clear knowledge" and "presumed knowledge". First of all, the "may know" view has uncertainty, and this uncertainty can limit the development of the information network industry. Many perpetrators of legitimate helping behaviors will not dare to develop and promote because they are afraid that their actions will be used by people with good intentions. We cannot let this uncertainty hold us back from legitimate acts of help. And this will make the scope of "knowing" too large, leading to the generalization of crime of assisting in information network-related criminal activities. Secondly, it is unreasonable to simply identify "knowingly" as "clearly knowing". This view, in turn, limits the subjective aspect too little. Because it is difficult to collect evidence on the subjective psychology of criminal suspects, this will lead to many criminals successfully escaping the punishment of the law. Special attention should be paid to the adoption of the "should have known" method of determining that "malicious should have known but did not know" does not belong to the connotation of "knowing". However, "what should have been known but known in bad faith" falls under the category of "knowingly", that is, the part of "ought to have known" belongs to "knowingly" [9].

3.2. Distinguish Between the Different Perspectives of the “Knowing” Object

The first view is that the "crime" must be a criminal act that meets the elements of the crime. The so-called criminal conduct that meets the constitutive elements of a crime, from the perspective of the four-element doctrine, is that it conforms to the object, objective, subject, and subjective aspects of the constitutive elements of a crime [10]. This makes it difficult to convict and is contrary to the original intent of the legislation for crime of assisting in information network-related criminal activities. For example, if the helper is a minor under the age of 14. In the case that the person being helped has not reached the age of criminal responsibility and therefore does not constitute a crime, if it is understood that the "crime" must be an act that meets the elements of the crime, then the helper cannot constitute crime of assisting in information network-related criminal activities. It is clear that this makes conviction more difficult. Some scholars believe that the crime of aiding and abetting has the characteristics of "one-to-many". This means that the act of helping alone is not socially harmful, but it acts as a link between many people who are helped. The social harmfulness of helping behavior should not be limited to a single person being helped, but should be viewed as a whole [11]. If "crime" is also understood as a criminal act that meets the elements of a crime, many acts of assistance will escape the punishment of the law.

The second view is that it is sufficient to understand "crime" as "ordinary illegal acts", which is an expansive interpretation that expands the scope of punishment. Adopting such a view would make it impossible for a large part of the population to recognize that their actions have constituted a crime. The adoption of this view may characterize as criminal offences ordinary offences that do not warrant criminal penalties. It expands the scope of punishment for aiding and abetting crimes, which may reduce crime of assisting in information network-related criminal activities to a "pocket crime".

The third view is that "crime" is an illegal act that meets the objective aspect of a specific crime [11]. This view is more reasonable, as the perpetrator only needs to recognize that the object of assistance is a criminal act. The perpetrator does not need to have a specific understanding of the specific charges, nature, or means of committing the crime. It should be noted that illegal acts that meet the requirements of the specific provisions of the Criminal Law and constitute objective elements of a certain crime, but are not subject to criminal punishment, are also included.

Under Section 115 of the New York State Penal Code, the crime of promoting crime is committed when the perpetrator believes that he or she is likely to be assisting another person who intends to commit the crime and that the means or opportunity he or she provides to commit the crime actually

DOI: 10.54254/2753-7048/57/20240094

helps that person to commit the crime. This provision of "crime promotion crime" also has a certain reference significance for China's judicial practice in the determination of "knowingly" crime of assisting in information network-related criminal activities. It does not require the perpetrator to have an understanding of the nature and means of the downstream crime aided by the aiding act, but only needs to recognize that the assisted person has the intent to commit the crime [12].

The establishment of crime of assisting in information network-related criminal activities is a kind of convictization of aiding and abetting, that is, he has become a new crime independently, rather than being treated as an accomplice to other crimes, and has an independent character [13]. Therefore, it is not necessary to have a specific and clear understanding of the downstream crimes, as long as it can be recognized that the "crime" it helps is a criminal act that meets the objective aspects of the crime, crime of assisting in information network-related criminal activities can be established.

3.3. The Pluralistic Standard of "Knowingly" is Determined in Practice

The determination of knowledge refers to how to determine that a criminal suspect subjectively has "clear knowledge". Clarification of how to determine "knowingly" is of great and far-reaching significance for theoretical research and judicial practice. It would be more appropriate to adopt a comprehensive approach to the identification of the subjective aspects of a criminal suspect. The so-called comprehensive approach is to combine objective evidence, the subjective confession of the criminal suspect, and whether the confession conforms to logic and facts.

When the defendant pleads guilty and accepts punishment, their confession is the main evidence of conviction. It actively expresses the state of subjective knowledge, which can be used as direct evidence to prove the basic facts of the case, but we cannot rely only on such verbal evidence, but also need to support each other with other objective facts to finally prove that the suspect has subjective "knowledge" of the crime. For objective recognition, reference can be made to the "Red Flag Principle". This principle is mainly applied to the determination of online infringement, which means that the behavior of the infringer is as obvious as holding a red flag in front of the service provider, and the network service provider cannot be unaware of the existence of such infringement [14].

When the defendant denies knowing it, due to the flexibility and difficulty in obtaining evidence of cybercrime, it becomes more difficult to determine the subjective "knowing" of crime of assisting in information network-related criminal activities without direct evidence. Article 11 of the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Criminal Cases Involving Illegal Use of Information Networks and Assistance in Information Network Criminal Activities clearly lists seven specific circumstances that can be deemed as "knowingly" committed by the perpetrator.

This provision reflects the presumption of knowledge. That is to say, in the absence of direct evidence to prove that the suspect is subjectively aware, combined with known facts and evidence, the judicial organ can infer that the suspect "knows" or "should know" that the helped person uses the information network to commit a crime. It should be noted that there is a certain possibility of error in the results obtained by this presumption method, so the situations listed in judicial interpretations cannot be directly used as the sole basis for determining the defendant's "knowledge". It is necessary to combine judicial interpretation and evidence facts to provide specific explanations and logical analysis of the case, in order to determine "knowing".

Moreover, in order to protect the legitimate rights and interests of suspect, it is necessary to ensure that suspect or defendants have the right to refute the presumption results. The so-called rebuttal is the ability to provide opposite evidence to prove one's innocence, which is actually a method of transferring the pressure of partial evidence from the judicial organs outward.

DOI: 10.54254/2753-7048/57/20240094

4. Conclusion

On the basis of continuous development and convenience brought to people's lives by information network technology, it is inevitable that it has become a breeding ground for criminal behavior due to its convenience, untraceability and other characteristics. In this context, crime of assisting in information network-related criminal activities provides the possibility of comprehensively rectifying the chain of information network crimes. There are also loopholes in the emergence of crime of assisting in information network-related criminal activities. Firstly, there is ongoing debate in the academic community regarding the meaning of "knowing", with different viewpoints. It is neither possible to limit the interpretation of "knowing" to "clearly knowing" which makes conviction difficult, nor to interpret it as "possibly knowing" which leads to the generalization of charges. It is more reasonable to combine "clearly knowing" and "should know". Secondly, for the determination of "knowing", subjective aspects should be combined with objective facts. When it is impossible to determine the subjective existence of knowing by the actor, the method of inferring knowing can be used. Finally, understanding "crime" as a "knowing" content as a "criminal act" that conforms to objective aspects is sufficient. Do not attempt to understand "crime" as a behavior that meets the requirements for constituting a crime, causing difficulties in criminalization, nor can "crime" be understood as a general illegal act, confusing illegality with crime. This study aims to provide useful ideas and insights for academic research and practical applications in related fields.

References

[1] *Majid, Y. (2013) Cyber crime and Society(2nd). Sage Publications.*

[2] *Zhaowu, W. (2021) Re-advocating the minimum accessory theory of accomplice: On the nature of the crime of assisting information network crime. Political and Legal Forum, 39(2),165-179.*

[3] *Claus Roxin. (2003) Criminal Law All Commoners(PartI). C. H. Beck Publications.*

[4] *Guisheng, C. (2007) A Study on the Elements of "Knowledge" in International Criminal Law: Taking Article 30 of the Rome Statute of the International Criminal Court as an Example. Legal Theory Series (Journal of Shanghai University of Political Science and Law), 5,64-69.*

[5] *Hong, L. (2017) On the Nature and Application of Crime of Assisting in Information Network-Related Criminal Activities. Legal application, 21, 33-39.*

[6] *(2020) Yu 0505 Xing Chu No.118.*

[7] *Yong, Z. and Jie, W. (2017) Helping in the "mastermind accomplice" and accomplice responsibility of information network criminal activities. Legal Theory Series (Journal of Shanghai University of Political Science and Law), 32(1),12-19.*

[8] *(2020)Yu 0191 Xing Chu No.1489.*

[9] *Xiao, W and Xinzhu C. (2023) The identification of " knowingly" in Crime of Assisting in Information Network-Related Criminal Activities. Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition), 25(6),50-58.*

[10] *Yunliang, S. (2019) Research on the Core Issues of Crime of Assisting in Information Network-Related Criminal Activitiess. Political and Legal Forum, 2,80.*

[11] *Yi, H. (2023) Research on Judicial Identification of Crime of Assisting in Information Network-Related Criminal Activitiess. Guangdong University of Finance and Economics.*

[12] *Su, J. (2020) The Interpretation Direction of Crime of Assisting in Information Network-Related Criminal Activities. Chinese Journal of Criminal Law, 5,76-39.*

[13] *Yanhong, L. (2016) Criticism on the Criminalization of Cybercrime Assistance Behavior. Legal and Commercial Studies, 33(3),18-22.*

[14] *Jiefeng, S. (2015) Identification of Trademark Infringement Liability of Network Service Providers—Also on Article 36 and Its Application. Intellectual Property Right, 5,11-19.*