Definition of the Presumption Rule of "Knowledge" in the Crimes of Assisting in Information Network-Related Criminal Activities

Yuanzhou Wu[1,a,*]

[1]*School of Civil and Commercial Law, Southwest University of Political Science and Law, Chengdu, Sichuan, China*

a. 1912211240@mail.sit.edu.cn

**corresponding author*

Abstract: The continuous development of network technology has profoundly transformed the daily production and lives of human beings. However, it has also given rise to numerous new forms of cybercrime, leading to the proliferation of certain cybercrimes. Assisting information network criminal activities constitute a crucial aspect of cybercrime. In 2015, the promulgated *Criminal Law Amendment (IX)* listed it as an independent offense. However, due to the problem of unclear judicial interpretation, the crime has been in a state of cold storage for a long time until 2019, when the Supreme People's Court and the Supreme People's Procuratorate promulgated *the Interpretation of a Number of Issues Concerning the Application of Law to the Handling of Criminal Cases of Illegal Utilization of Information Networks and Helping Criminal Activities on Information Networks and Other Criminal Cases* the crime has gradually begun to be applied in large quantities. In recent years, the crimes of assisting in information network-related criminal activities has been on the rise, but there have been numerous objections and lack of consensus regarding the determination of subjective knowledge in judicial practice and the theoretical community. Therefore, it is crucial to clarify the presumption rule of knowledge to provide guidance for judicial practice.

Keywords: cybercrime, information network criminal activities, subjective knowledge, presumption rule, relecommunications fraud

1. Introduction

In the era of Internet 3.0, network technology has penetrated into all aspects of the public's daily life, because the public does not understand the emerging network technology comprehensively enough, and the innovation of technology will trigger the innovation of law [1]. Helping information network crime is a typical example. Information network crime is a new type of crime, but it has caused great trouble to people's daily life, and it is of great significance to fight against helping network information crime. However, there have been many discussions in the academic circle regarding the interpretation of "knowledge" in this crime, and the phenomenon of "different judgments in similar cases" has also emerged in judicial practice, thereby impacting the fairness of the decision. In response to this, in 2019, the Supreme People's Court and the Supreme People's

Procuratorate Procuratorate issued *the Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Utilization of Information Networks and Helping Criminal Activities on Information Networks* (*the Interpretation of Helping Criminal Activities on Information Networks*). Furthermore, with the implementation of the "two cards" campaign in judicial practice, a significant number of activities involving the acquisition, leasing, and sale of "two cards" have been criminalized and sentenced as crimes of assisting information networks (crimes of assisting in information network criminal activities). The crimes of assisting in information network-related criminal activitieshas been criminalized and sentenced. However, many disagreements have arisen in judicial practice regarding the issue of subjective knowledge. For instance, prior to the introduction of *the Interpretation of Helping Criminal Activities on Information Networks*, leading to uncertainty among courts at all levels in different regions regarding its determination. Although *the Interpretation of Helping Criminal Activities on Information Networks* provided more detailed rules on the presumption of knowledge, there were significant issues in the determining the knowledge of the crime in judicial practice. Specifically, the scope of "should know" was not entirely consistent, and a considerable number of judgments did not provide a clear definition of subjective knowledge or reason about it. Therefore, it is necessary to further clarify the meaning of "knowingly," particularly in defining the rule of presumption of knowledge, in order to provide theoretical support for judicial practice.

2. Provisions on "Knowledge" in Existing Legislation on the Crimes of Assisting in Information Network-Related Criminal Activities

Article 287 of the Criminal Law stipulates that "Anyone who, knowing that another person is using an information network to commit a crime, provides technical support such as Internet access, server hosting, network storage, communication transmission, or assistance such as advertisement and promotion, payment and settlement, and where the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and shall be fined concurrently or singly." From this, it can be seen that "knowledge" is the subjective cognitive element of the crimes of assisting in information network-related criminal activities.

On November 1, 2019, *the Interpretation of Helping Criminal Activities on Information Networks* issued by the Supreme People's Court and the Supreme People's Procuratorate came into effect. *The Interpretation* further defines the concept of "knowingly" in the crimes of assisting in information network-related criminal activities. It specifies certain circumstances where the presumption of knowledge can be made. These circumstances include: (1) Abnormal transaction price or method; (2) Providing programs, tools, or other technical support intended for illegal activities; (3) Frequently adopting measures such as hidden access to the Internet, encrypted communications, data destruction, or using false identities to evade supervision or investigations; (6) Assisting others in evading supervision or investigations; (7) Other circumstances that can sufficiently establish the perpetrator's knowledge. It is important to note that item (7) provides flexibility for future developments in the network environment, allowing for additional circumstances where knowledge can be presumed.

However, Article 9 of *the Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases of Telecommunications Network Fraud and Other Criminal Cases* (II) *(the Opinions on Several Issues Concerning Network Fraud*), jointly issued by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security in 2022 states that "if a person knows that another person is using the information network to commit a crime and provides any of the following forms of assistance in committing that crime, it can be deemed as "other serious circumstances" as stipulated in Item (vii) of Paragraph 1 of Article 12 of *the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on*

Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving the Illegal Use of Information Networks and Assistance in Criminal Activities on Information Networks, etc.: Acquiring, selling, or renting credit cards, bank accounts, non-bank payment accounts, internet account passwords with payment and settlement functions, network payment interfaces, or online banking digital certificates, exceeding five (5); (b) Acquiring, selling, or renting other people's SIM cards, traffic cards, or Internet of Things cards, exceeding twenty (20). It is evident that the Opinions on Several Issues Concerning Network Fraud not only supplements the enumeration in item 7 of *the Interpretation of the Application of Law in Handling Cases of Assisting Criminal Activities on Information Networks* but also demonstrates its forward-thinking and scientific nature.

However, from a textual interpretation perspective, it is not difficult to see that *the Interpretation of Helping Criminal Activities on Information Networks* does not provide a clear definition of "knowledge" in the crimes of assisting in information network-related criminal activities

Although *the General Provisions of the Criminal Law* have made general provisions on "knowledge", the sub-principles of *the Criminal Law* specially emphasize the subjective knowledge of the perpetrators in certain criminal acts. Among them, there are a total of 45 provisions on "knowledge" in the sub-principles of *the Criminal Law*, and Article 219 (2) of *the Criminal Law*, which pertains to the crime of infringing on trade secrets, must be particularly noted. The crime of violating trade secrets is expressed as "knowing or should know" in terms of subjective intent. However, *the Amendment (XI) to the Criminal Law*, which came into effect on March 1, 2021, removed this expression and unified the use of "knowledge" for subjective intent in *the Criminal Law*.

In addition, some judicial interpretations stipulate that knowledge includes "knowing or should know". The earliest provision appeared in *the Interpretation on Several Issues Concerning the Specific Application of Law in Handling Theft Cases*, issued by the two high courts in 1992. Although *the Interpretation* was repealed in 2013, the provision that knowledge includes "should know" has been incorporated and used by several subsequent judicial interpretations and widely applied in judicial practice. For example, Article 5(2) of the 2017 *Interpretation of the Two High Committees on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens' Personal Information* stipulates that "a person who knows or should know that another person has used citizens' personal information to commit a crime, and sells or provides it to him or her" shall be deemed to have "aggravating circumstances". The provisions on knowledge in these judicial interpretations largely imply a presumption of "should have known". Similar to *the Amendment (XI) to the Criminal Law*, *the Interpretation of the Two High Committees on Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Networks and Helping Criminal Activities on Information Networks* (*the Interpretation of Helping Letters*) does not specifically state that the subjective knowledge includes the phrase "should have known". The specific expression is as follows: "except where there is evidence of explicit ignorance." In summary, *China's Criminal Law* and relevant judicial interpretations regarding the definition of "knowingly" are not uniform. This is why there continues to be controversy in theoretical and practical circles. This paper aims to define the presumption of "knowingly" rules and attempt to establish a basis for defining the presumption rule of "knowledge" in the crimes of assisting in information network-related criminal activities.

3. Construction of the Presumption Rule of "Knowledge" in the Offense of Helping Information Network Criminal Activities

3.1. Interpretation of Knowledge

The understanding of "knowledge" in the crimes of assisting in information network-related

criminal activities determines certain aspects of the offense and its punishment, as well as the construction of the presumption rules in judicial practice.

Different scholars hold different views on this matter. For instance, some scholars believe that regarding the crimes of assisting in information network-related criminal activities, the criminal law system should take a cautious approach when determining "knowledge." This can help alleviate judicial controversies surrounding the offense. If the interpretation of "knowledge" in the crimes of assisting information network-related criminal activities includes "should know" or "may know," it may undermine the principles of criminal law and punishment. Moreover, it may raise questions about the limits of judicial discretion. Considering the consistent approach of the criminal law system in determining knowledge, it is not appropriate to include "should know" or "may know" within the scope of knowledge for the crimes of assisting in information network-related criminal activities. Doing so would lower the threshold for criminalization, ultimately expanding its regulatory scope under criminal law. Otherwise, the threshold of criminalization for the crimes of assisting in information network-related criminal activities will be lowered, leading to an unlimited expansion of the scope of criminal law [2]. Based on this, scholars believes that "knowledge" in the crimes of assisting in information network-related criminal activities should solely refer to "actual knowledge" and should not include the concept of "should know".

Some scholars have presented different perspectives on this matter. For instance, some scholars argue that adopting the concept of "should know" can help address the evidentiary challenges in proving "knowledge" in judicial practice, specifically by employing legal presumptions. By utilizing legal presumptions, the "knowledge" of the aider can be established. On the other hand, some other scholars believe that the legislative intent of this crime is to criminalize the act of aiding, which implies a "criminalization" approach. Including "should know" within the definition of "knowingly" would also encompass negligence and attract penalties. However, the provisions of this crime do not explicitly stipulate punishment for negligence, which can be seen as an expansion of incorrect application. In reality, this is not entirely accurate. Firstly, the "should know" aspect of this crime pertains to what the aider "should have known" or "should have been aware of", which brings forth the notion of "presumed knowledge". Presumed knowledge refers to the cognitive element of an intentional offense. It encompasses the idea that, based on common sense, logic, and societal values, the aider "should have known but did not know". Determining whether this knowledge is present requires specific analysis of individual cases, taking into account the presumption of knowledge. Secondly, the logical premise of "should have known" is the absence of actual knowledge. It does not involve the subjective aspect of foreseeing whether the assisted person will commit the crime. Conversely, an aider who "should have known" about the actions of the assisted person demonstrates a level of caution that an average person could reasonably achieve. Therefore, it is unrelated to criminal negligence [3].

The concept of "knowledge" in criminal law is indeed somewhat ambiguous. This paper argues that the concept of "knowledge" in the offense of aiding information network criminal activities should encompass both actual knowledge and constructive knowledge ("should know"). The inclusion of "should know" in the definition of "knowledge" is a topic of contention among scholars. For instance, some scholars believe that it is reasonable and feasible to include "should know" within the scope of "knowledge" in the offense of aiding information network criminal activities. From a legal standpoint, "knowing" in this context overlaps with both actual knowledge and constructive knowledge, and "should know" falls under the category of knowledge in judicial determination. Moreover, although may be variations in terminology across different periods of interpretation, the underlying connotation remains consistent and generally encompasses both actual knowledge and constructive knowledge. In recent years, judicial interpretations have consciously avoided explicit references to the controversial terms "know" and "should know", instead placing

greater emphasis on evidence-based reasoning to determine whether the perpetrator acted "knowingly". This shift indicates a move towards inferring knowledge, and in nature, there is no substantial difference between inferring knowledge and the concept of "should know". In essence, "know by inference" and "should know" are fundamentally the same. From the perspective of legislative objectives, the establishment of the offense of aiding information network criminal activities is driven by significant practical considerations. With the rise of cybercrime as a mature and pervasive industry, providing assistance such as venues, tools, technical support, and other forms of support constitutes the initial stage of the cybercrime chain and carries severe harm. If "knowingly" only refers to actual knowledge and did not include constructive knowledge, it would place an excessive burden of proof on judicial authorities, potentially allowing some criminals to evade criminal liability. This outcome would not conducive to Combating cybercrime [4].

The legislature and judiciary have indeed developed certain understandings regarding this matter. In *the Criminal Law Amendment (IX)*, when introducing the provision on the offense of aiding information network criminal activities, the legislature took into consideration the challenges associated with prosecuting individuals involved in cybercrime under the existing provisions on complicity in the criminal law. For instance, when treating such offenses as joint crimes, it becomes necessary to establish the accomplice's intent to commit the crime. However, in reality, individuals involved in different stages of the criminal activity may not know each other and there may be no clear evidence of their direct communication or shared criminal intent [5]. If we do not focus on the existence of intentional communication between the accomplice and the perpetrator of the information network crime, the subjective element of the offense of aiding information network criminal activities - namely, "knowledge" - will primarily rely on assessing the subjective understanding of the accomplice alone. Based on this perspective, judicial authorities tend to interpret "knowingly" as encompassing clear knowledge, potential knowledge, and constructive knowledge, which can alleviate the difficulties faced by judicial authorities in verification through presumptions and inferences. Empirical research findings indicate that in a sample of 1,081 judgments related to the offense of aiding information network criminal activities, the percentage of defendants mentioned by the court as having "actually knowing" (45.1%) and those mentioned as potentially having knowledge (54.2%) were similar [6]. It is foreseeable that if the judicial practice only confines "knowledge" to explicit knowledge, there will be a significant number of cases that are difficult to conclude.

This paper argues that in the offense of aiding information network criminal activities, "knowledge" should encompass both explicit knowledge and constructive knowledge ("should know"). Although *the Interpretation of Helping Information Network Criminal Activities* does not explicitly define "knowingly," certain judicial interpretations stipulate that "knowingly" includes both actual knowledge and constructive knowledge ("knowing or should know").

Second, from the perspective of purpose interpretation, telecommunication network fraud is a new type of cybercrime that has been highly prevalent in recent years. The Central Committee of the Communist Party of China, with Comrade Xi Jinping at its core, attaches great importance to the efforts in combating and managing illegal and criminal activities related to telecommunication network fraud. General Secretary Xi Jinping has issued important instructions on multiple occasions. On April 9, 2021, General Secretary Xi Jinping issued an important instruction emphasizing that "in recent years, all regions and departments have implemented the decision-making and deployment of the Central Committee of the Party, and have continued to carry out the fight against and management of telecommunication network fraud, achieving initial results. To adhere to the people-centered approach, integrated development, and security, strengthen the system concept, rule of law thinking, focus on the root causes of governance, and comprehensively govern. Adhere to coordinated efforts, population control, fully implement measures to combat, prevent, and control,

and strengthen the main supervisory responsibility in the financial, telecommunications, internet, and other industries. Strengthen the social publicity, education and prevention, promote international cooperation in law enforcement, and resolutely curb the trend of the occurrence of high incidence of such crimes, the Make new and greater contributions to building a higher level of peaceful China and China under the rule of law." The use of telephone cards and bank cards to commit telecommunication network fraud has been strongly condemned by the public, and media reports have also highlighted the significance of judicial authorities in combating telecommunication network fraud during this period.

The division of labor in the crimes of assisting in information network-related criminal activities greatly influences how judicial authorities can distinguish between the subjective and objective elements of the crime. In judicial practice, it is evident that this crime is closely related to telecommunication network fraud compared to other information network criminal activities. Based on the prosecution data of the Supreme People's Procuratorate in the first half of 2022 for the crime of assisting in information network-related criminal activities, the upstream crimes supported by this offense were primarily concentrated in the areas of telecommunication network fraud and online gambling. The illegal trading of "two cards", especially bank cards, which provided the tools for payment transfers, cashing out, and withdrawals, accounted for more than 80% of the total number of prosecutions [7]. It can be stated that the cracking down on criminal activities in the information network is not only an important measure for implementing the instructions of the General Secretary but also a practical necessity to address the security concerns of the people and enhance their sense of well-being.

Helping information network criminal activity is a crucial aspect of telecommunication fraud. Strengthening the fight against helping information network criminal activity is of significance importance in effectively combating telecommunication fraud, safeguarding people's live and property, and creating a "clean" cyberspace. Therefore, this paper disagrees with the notion that "knowingly" in the crimes of assisting information network-related criminal activities should only be interpreted as "clear knowledge." Such an interpretation would undeniably increase the burden of proof for judicial authorities and hinder the fight against this crime. Conversely, "knowledge" should encompass both actual knowledge and what a person should reasonably know.

3.2. Construction of the Criminal Presumption Rule of "Knowledge" in the Crimes of Assisting in Information Network-Related Criminal Activities.

It is necessary to standardize the establishment of rules regarding "knowledge" in the crimes of assisting in information network-related criminal activities.

First and foremost, the construction of the criminal presumption rule of "knowledge" in the crimes of assisting in information network-related criminal activity must align with the leniency and severity principles of criminal policy. It should comprehensively and accurately implement the leniency aspect of the criminal policy by strictly following the law and imposing strict punishments when necessary, while also upholding the importance of accuracy. On the one hand, it is crucial to unwaveringly adhere to the principle of being "strict" and impose severe punishments on individuals involved in serious crimes. This will ensure that society feels the deterrent force of strict enforcement, thereby enhancing the people's sense of security. On the other hand, the lenient aspect should be standardized, ensuring that lenient policies are implemented strictly in accordance with the law for minor offenses. According to the Procuratorate Daily, in the first half of the year, a total of 316,000 criminal suspects of various types were arrested, indicating the commitment to combating the crimes of assisting in information network criminal activities and creating a safe cyberspace to protect people's lives and property [8]. It is of great significance to uphold the law in combating the crimes of assisting in information network-related criminal activities, prevent it from

becoming a prevalent offense, and create a secure cyberspace for the protection of people's lives and property.

Secondly, the construction of the presumption rule of "knowledge" for the crimes of assisting in information network-related criminal activities should incorporate a combination of specific enumeration, a pocket clause, and an exclusion clause. Alongside the existing six paragraphs in the judicial interpretation, future cases should be specifically enumerated to address new types and situations that may emerge. This approach is necessary due to the evolving network environment, where people's understanding is not only based on traditional knowledge but also influenced by rapid advancements in network technology. For instance, the emergence of ChatGPT has altered people's conventional understanding of artificial intelligence. However, it is important to note that certain unscrupulous individuals may exploit the functions of ChatGPT to commit cybercrimes. Therefore, it is crucial to establish a comprehensive framework that encompasses specific examples, incorporates a flexible clause to cover emerging scenarios, and includes an exclusion clause to avoid misapplication. This will ensure the effective detection and prosecution of individuals involved in helping information network criminal activities, safeguarding the integrity of cyberspace, and protecting society from potential harm.

Third, it is important to acknowledge that the presumption rule of "knowingly" may not encompass every possible case. In specific instances, even if there is no explicit enumeration in judicial interpretations, practitioners can rely on their experience in handling similar cases to make a presumption of knowledge based on equivalent circumstances. If the evidence indicates that the perpetrator should have known, the establishment of the crimes of assisting in information network-related criminal activities can be supported [9]. For example, in practice, there are cases where perpetrators intentionally evade regulatory measures when assisting information network criminal activities. For example, they may withdraw money on behalf of others while taking elaborate precautions to avoid surveillance cameras at ATM machines. In such situations, the perpetrator's subjective knowledge can be presumed based on their deliberate attempt to circumvent regulatory measures. Another scenario is when law enforcement officers are investigating a crime, and the perpetrator takes actions to destroy evidence or warns the suspect about the ongoing investigation. In such cases, the perpetrator's subjective knowledge can be presumed based on their behavior of evading investigation and providing information to the suspect after the commission of the crime. Furthermore, if the individual withdrawing money possesses multiple bank cards with different account holders or multiple fake ID cards and is unable to provide a convincing explanation, it can also lead to the presumption of their subjective knowledge. These examples demonstrate that subjective knowledge can be inferred from the actions and behaviors of individuals involved in assisting information network criminal activities, even in the absence of explicit enumeration in judicial interpretations [10].

Fourthly, the paper suggests that the construction of the presumption rule of "knowledge" in the crimes of assisting in information network-related criminal activities should involve consultations with public security authorities. The crimes of assisting in information network-related criminal activities falls under the category of new and complex crimes, requiring judicial bodies to accumulate more experience, conduct targeted research and development of investigative technologies, and enhance the expertise of their personnel. Currently, front line investigators still encounter significant challenges in handling such cases. These challenges include difficulties in discovering relevant clues, retrieving evidence, and countering the strong investigative capabilities of criminals. Therefore, it is crucial for judicial organs to collaborate closely with public security authorities to address these difficulties and develop effective strategies for investigating and prosecuting cases related to assisting in information network criminal activities [11]. The construction of the "knowing" presumption rule should also be linked with the public security

investigative authorities to form a synergy between the public security and judicial authorities in order to better combat crime and better protect the people's property.

4. Conclusion

The subjective knowledge of the crimes of assisting in information network-related criminal activities is vague, the objective helping behavior is ill-defined, and the threshold of incrimination is low, which leads to the fact that the crimes of assisting in information network-related criminal activities inherently contains the gene of "pocketing", and therefore needs to be substantively interpreted before applying the crimes of assisting in information network-related criminal activities. The core essence of national governance lies in institutional governance, especially the institutionalized governance system centered on the pursuit of good law and good governance. Based on this, the core viewpoint of this paper is that "knowledge" in the crimes of assisting in information network-related criminal activities should be understood as both "actual knowledge" and "should have known". When constructing the presumption rule of "knowledge", it is necessary to adhere to the criminal policy of balancing leniency and severity. The construction of the presumption rule of "knowledge" for the crimes of assisting in information network-related criminal activities should also establish the mode of "specific enumeration + underlining provisions + exclusion clauses". focus on achieving crime and punishment but also exercise discretion based on the evidence. They should protect the legitimate rights and interests of the perpetrators of crimes while ensuring the severe punishment of criminals. By doing so, they can effectively reduce the occurrence of assisting information network criminal activities and minimize the crime rate in China.

References

[1] *Bijan F.M. (2022) Innovative Liability in Criminal Law: Between Strict Liability, Negligence and Allowable Risks. translated by Tang Z., Soochow University Journal of Law, 3, 48-61.*

[2] *Liu Y. (2023) The Judicial Expansion Trend and Substantial Limitation of the Offense of Helping Criminal Activities on Information Networks. China Law Review, 3, 58-72.*

[3] *Zeng L. (2023) The Judgment Logic and Scope Limitation of "Knowingly" in the Crimes of Assisting in Information Network-Related Criminal Activities. Journal of the Chinese People's Public Security University (Social Science Edition), 1, 64-71.*

[4] *Yin Z. (2023) The Understanding and Application of "Knowingly" in the Crimes of Assisting In Information Network-related Criminal Activities. Citizen's Law (Comprehensive Edition), 4, 32-42.*

[5] *Zang T. (2015) Interpretation of Amendment (IX) to the Criminal Law of the People's Republic of China. Legal Publishing House, 210.*

[6] *Zhou Z., Zhao C. (2022) An Empirical Study on the Crimes of Assisting in Information Network-Related Criminal Activities" - Taking 1,081 Judgments as a Sample. Applying the Law, 6, 83-93.*

[7] *Dai J., Zhao X. (2022) Procuratorial Organs Prosecute 64,000 People for the Crime of Helping Information Network Criminal Activities in the First Half of the Year. Procuratorial Daily, 23, 1.*

[8] *Procuratorate D. (2023) A total of 316,000 criminal suspects of all types were arrested in the first half of the year. Retrieved from . http://newspaper.jcrb.com/2023/20230720/20230720_004/20230720_004_3.htm.*

[9] *Research Group of Beijing Municipal Daxing District People's Procuratorate. Research on Difficult Issues of Judicial Practice on the. Crimes of Assisting in Information Network-Related Criminal Activities" Research on the Prevention of Juvenile Delinquency, Retrieved from 42-49.*

[10] *Yu H. (2021) Twenty Lectures on Cybercrime. Law Press·China, Sixth Edition, 104.*

[11] *Luo M., Zeng J. (2022) Analyzing the Difficulties in Investigating Cases of Helping Information Network Crimes and Investigative Countermeasures. Guangzhou Municipal Public Security Management Cadre College Journal, 2,10-16.*