Analysis of the Recognition of "Clearly Knowing" in the Crime of Assisting Information Network Criminal Activities Based on Chinese Payment Methods

Wenyan Xiao[1st,a*], Yequan Zhang[1st,b]

Southwest University of Political Science & Law, Law & International Economics and Trade, Chongqin, China
These authors contributed equally to this work and share first authorship.

[a*]3288431898@qq.com, [b]1473524903@qq.com

Abstract. This article sorts out the three views in the academic community on the interpretation of the "actual knowledge" element in Article 287 of the Criminal Law on the crime of assisting information network criminal activities: the narrow view, the plain view, and the broad view. The author compares the three views in terms of punishment justice and judicial efficiency, and believes that "actual knowledge" should adopt the interpretation of "clearly knowing or should have known", so as to adapt to the goal of the crime establishment: cutting off the chain of benefits of network crime. Based on the comparison between real judicial cases and the content of non-prosecution decision letters, the author summarizes two standards used in judicial practice to judge the extradition and incrimination of the crime of helping information network crime activities. In combination with the current situation of China's crime of helping information network crime activities, it proposes suggestions for improving the identification system of "should have known" from the perspective of helping the crime of information network crime, and puts forward new views on market supervision improvement, market subjects' transaction obligations and crime information notification.

Keywords: assisting information network criminal activities; clearly knowing; should have known; might have known.

1 Introduction

The crime of assisting information network criminal activities (hereinafter referred to as the crime of assisting information network criminal activities) is a new charge added in the Ninth Amendment to the Criminal Law. It equips the act of assisting in network crimes that infringe on legal interests with independent statutory charges and penalties, in order to curb the rampant development of network crimes. In October 2019, 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 Involving Illegal Use of Information Networks and Assistance in

Z. Zhan et al. (eds.), *Proceedings of the 2024 10th International Conference on Humanities and Social Science Research (ICHSSR 2024)*, Advances in Social Science, Education and Humanities Research 858,
https://doi.org/10.2991/978-2-38476-277-4_193

Information Network Crimes" (hereinafter referred to as the "Interpretation"), which stipulated the determination of the core constituent elements of the crime of assisting information network criminal activities, and the judgment cases of assisting information network criminal activities showed a rapid development. According to data from China Judgment Document Network (https://wenshu.court.gov.cn/). In 2019, the number of convictions for the crime of assisting information network criminal activities increased from 192 to 3246 in 2020, and then to 22412 in 2021, 11264 in 2022, and 10461 in 2023. Currently, it has become the third most prosecuted crime among all types of criminal offenses (the top two being the crime of dangerous driving and theft). And in Latin America, Anna pointed out that cyberattacks have been on the rise for years before the Covid-19 pandemic as well, but the quarantine, the changing living conditions of citizens, and traveling restrictions increased the cyberattacks against nations as the citizens relied on the online services more.[1] Meanwhile, in the USA, Though research examining cybercrime has surged in recent years, studies exploring perceptions concerning these phenomena have been scant. In fact, little is known regarding the extent to which individuals perceive cybercrime as serious, whether exposure to cybercrime terminology elicit similar perceptions of seriousness as behavioural descriptions of cybercrime, and the factors predicting perceptions of cybercrime seriousness.[2] Due to the lowering of the threshold for determining "clearly knowing" in judicial practice, judges have been given a greater range of discretion, resulting in situations where it is easy to incriminate and difficult to incriminate for the crime of assisting information network criminal activities. This is an improper expansion of punishment, increasing coverage and impact. Professor Chen Hongbing believes that there is a risk of the number of cases sentenced for the crime of assisting information network criminal activities increasing rapidly in recent years. This is manifested in the fact that it is easy to be convicted and difficult to be convicted. To correct this phenomenon, it is necessary to pay attention to the determination of the core element of establishing the crime of assisting information network criminal activities, which is "clearly knowing". The academic community has made many explorations in this regard. Professor Zhang Tiejun pointed out that the regulation of clearly knowing content should clarify the intervention boundary of network neutral behavior, and "clearly knowing" should be limited to the scope of actual knowledge and reasons or the ability to know; Professor Pi Yong believes that knowledge should be presumed to be known by the actor, without involving the obligation of the actor to foresee the consequences of the behavior, but emphasizing the state of knowledge; Professor Zhang Mingkai believes that knowing does not include knowing what should have known, and requires a distinction between knowing what may and might have known. However, academic debates still face difficulties in implementation due to the fact that they often involve concepts and boundaries in theory, without further implementation measures, without constructing judicial standards that implement these principles in practice, and without further connection to specific judicial practices. This article attempts to further refine and concretize the standards of knowledge from 1029 non prosecution opinions in China, so that the theoretical "knowledge" can be beneficial for exploring and deeply guiding judicial judgments, promoting better

application of the crime of assisting information network criminal activities, and reflecting the modesty of criminal law.

2 Viewpoints and Choices of Clearly Knowing on the Crime of Assisting Information Network Criminal Activities

In the academic community, there is much debate about the meaning of the constituent elements of the crime of assisting information network criminal activities, such as the viewpoint that "clearly knowing" should be "clearly knowing, indeed knowing" [3]. This viewpoint requires judicial authorities to confirm that the perpetrator has a precise understanding of the criminal act committed by others rather than a general understanding when determining "clearly knowing"; There are also views that believe that the meaning of "clearly knowing" is "clearly knowing and might have known" [4], which means that when determining whether the perpetrator constitutes "knowing", only the perpetrator is required to have the possibility of knowing the criminal act committed by others, and may have a general understanding of the criminal act committed by others; There is also a viewpoint that "clearly knowing" means "clearly knowing and should have known" [5]. This viewpoint believes that, apart from having a clear understanding of the criminal illegality of the behavior committed by others, when starting from a factual basis, if the perpetrator is likely to know that the behavior they are assisting in is a cybercrime and wishes or allows it to occur, it is presumed that the perpetrator constitutes "clearly knowing". For the first viewpoint, we believe that the original intention of establishing the crime of assisting information network criminal activities is to cut off the chain of cybercrime, which is a light crime, and its sentencing level is less than three years. If the perpetrator has a clear understanding of the cybercrime they helped and still chooses to provide different types of help or support, it should be regarded as accomplice. At the same time, if evidence is required to prove that the perpetrator has a clear understanding of the behavior they helped, it may mean that the difficulty of evidence investigation and the threshold for prosecution by public security and procuratorial organs have increased, making it difficult for the crime of assisting cybercrime to effectively combat such behavior, which is contrary to the original intention of establishing this crime; For the second viewpoint, we believe that expanding the definition of "knowing" to "knowing" may lead to improper expansion of the coverage area of criminal law, which goes against the modest goal of criminal law. That is to say, "knowing" as an optional fuzzy cognitive state conflicts with the certainty of criminal law. Using "might have known" as "clearly knowing" would make the crime of assisting information network criminal activities become a "pocket crime".

The author believes that the third viewpoint is more appropriate, as "should have known" serves as a supplement to "exact knowledge", which is conducive to the comprehensive crackdown on the assisting behavior of cybercrime by the crime of assisting information network criminal activities. It also limits the generalization of the crime of assisting information network criminal activities, and has an effect on the trend of the chain and industrialization of cybercrime in China. However, in the aca-

demic community, it is still a controversial topic to determine the criteria for "should have known" in judicial practice. Furthermore, the boundary issue between "should have known" at the judicial level and "might have known" in daily life is still worth exploring. The application of what should have known is an expansion of the boundaries of criminal law and a choice made based on judicial efficiency. Therefore, we strive to make "should have known" subject to reasonable limitations of human rights protection to prevent improper expansion. [6]

To this end, we studied 1029 opinions on the non prosecution of crimes related to assisting online information activities (i.e. all relevant opinions in 2023 and 2022) on the magic weapon of Peking University. Starting from the comparison of the specific circumstances of the crime of assisting information network criminal activities and its inclusion, we attempted to analyze under what circumstances "clearly knowing" can be recognized in real judicial practice, and attempted to provide a unified standard for the identification of "clearly knowing" evidence or a feasible plan, in order to obtain an analysis and summary of the standards and factors for the identification of "clearly knowing" in assisting information network criminal activities crimes. We discussed the boundary limitations of "should have known" in the perspective of assisting information network criminal activities crimes. On this basis, we can explore how to better improve the non prosecution system in China, in order to improve the application system of the crime of assisting information network criminal activities.

3 Relevant Perspectives on "Should Have Known" in Theoretical Research

Article 14 and 15 of the Criminal Law provide for two situations of subjective responsibility. Article 14 states that "if one knows that one's behavior will result in harmful consequences to society, and wishes or allows such consequences to occur, thus constituting a crime, it is an intentional crime. Intentional crime should bear criminal responsibility. Article 15 states that" one should foresee that one's behavior may result in harmful consequences to society, but if one did not foresee due to negligence or believed that such consequences could be avoided due to negligence, it is a negligent crime. "When applying this charge to the crime of assisting information network criminal activities, one should first exclude the situation of negligence or being deceived, as well as the situation of being deceived and believing in avoiding such consequences."; The second point is that we have achieved considerable results in defining "should have known" in academic discussions.

Some scholars believe that starting from the determination of time, it is possible to conduct a link examination before, during, and after to determine whether the perpetrator is likely to understand that the behavior committed by others is a criminal act, thereby ensuring that the presumption of "should have known" evidence is more reliable [7], that is, to determine the state of clearly knowing, more attention should be paid to the details of the suspect before and after. Therefore, we will examine the prior details that courts should focus on when making judgments, and how we can

appropriately adjust our expectations of cognitive abilities for specific groups of people, such as third-party platform sublessors.

Starting from the classification of evidence, some scholars believe that "should have known is a presumed knowledge, and the judicial authorities still have sufficient evidence for the defendant's proof of clearly knowing, but have not received confirmation from the defendant." [8], in fact, it emphasizes that the positioning of the "confirmation" content in China's determination of clearly knowing should not be too high. Therefore, the author believes that the extension of the term "sufficient evidence" should be partially defined, and the content of effective evidence in two card crimes will be discussed in the following text.

Some scholars believe that it should have known that it includes situations such as "inferring the perpetrator's knowledge based on the specific content of the assistance provided, and inferring the perpetrator's knowledge based on multiple offers of assistance, which can prove the perpetrator's malice." [9] However, we believe that in the crime of assisting others, "one should have known" is essentially that the perpetrator is likely to recognize that the act they are helping is legally harmful and knows that their helping behavior will cause social harm. That is to say, theoretical considerations should be based on the two aspects of the actor's cognition. Firstly, whether they have a sufficient understanding of the illegality of the behavior they help with. The "full understanding" here does not require the actor to have a specific understanding of the type of crime or the process of crime committed by others, but rather a general understanding of the social harm or infringement of the said helping behavior. In other words, based on the essence of the crime as the standard, as long as they recognize that the implementation of the behavior will harm social interests and there is a risk of violating the law, it is sufficient; The second is to have an understanding of the potential harm that the helping behavior one is carrying out. This requires the perpetrator to have a direct understanding of the social harm that the helping behavior they are about to carry out or are currently carrying out may cause. In other words, it is likely that the behavior will be used for criminal activities, and if one does not carry out the helping behavior, it will not help generate social harm. For the former, it can be examined from the degree of participation of the perpetrator in the process of committing cybercrime by others, whether there is interesting contact, and the communication object. The "should have known" and "should have known" still require starting from the normal level of understanding of an ordinary person (specific description of case analysis in the following text). For the latter, we can make a preliminary examination from the specific content of the help provided by the actor, the number of times the help was provided, whether the benefits were obtained from the help behavior, whether the source of the benefits was understood, whether the help behavior was actively implemented for the benefit, professional background, educational level, etc., and then measure whether the actor had specific and suitable conditions or environment to make the actor aware during the process of providing help. For example, in the case of Xing's assistance in information network criminal activities, the suspect signed the "Notice on Suspected Illegal Activities in Selling, Lending, Renting Mobile Cards, Bank Cards, Identity Documents, Corporate Accounts, etc." when applying for a bank card, which can be considered that the perpetrator has

some understanding of the payment and settlement assistance provided by the network crime, and belongs to the situation of "clearly knowing".

4 Comparison of the Determination of “Should Have Known” in Judicial Practice

According to the data collected by Peking University's Treasure, there were a total of 1029 non prosecution opinions on the crime of assisting trust in 2023 and 2022. After screening by the author, only nine cases were explicitly mentioned in the judgment because the prosecutor's office believed that the perpetrator did not constitute a clear understanding of the situation and escaped the crime. The vast majority of non prosecution cases were based on significantly minor criminal circumstances, with suspects being first-time or occasional offenders. In addition, there were also a small number of non prosecution cases where the verdict was changed to cover up or conceal the crime, or fraud and insufficient evidence were ultimately released. Compared to the judicial judgments on the crime of assisting information network criminal activities in 2022 and 2023, the non prosecution opinion appears to be rare, and in the opinion, the non prosecution opinion due to insufficient evidence for "clearly knowing" the circumstances is even more insignificant. However, it is in such cases that we see the cautious investigation and judgment of judicial personnel and the careful exploration of the boundary of the constitutive requirement of clearly knowing.

After comparing the determination of "clearly knowing" in cases where the crime of assisting information network criminal activities is committed or committed, the author believes that the following standards can be used in judicial practice to distinguish between "should have known" and "might have known".

4.1 The "Notification" in the "Interpretation" Should Adopt the Explanation of "Specific Content Notification"

In the case of Gao et al.'s assistance in information network criminal activities [10], when Gao et al. were helping to unblock accounts suspected of committing crimes, they received a clear warning from WeChat that "the account may be suspected of online fraud". However, after realizing the risks, Gao et al. still chose to help unblock illegal accounts for economic gain. Therefore, the People's Court of Jianggan District, Hangzhou City, Zhejiang Province, determined that Gao and others constituted a "clearly knowing" situation. In other words, from the perspective of the general public's level of understanding, when Gao and others learned that their help to unblock accounts may be suspected of illegal activities, they should be vigilant. Although the official WeChat prompt is possible, multiple accounts that Gao and others are about to unblock have this prompt, so it should be recognized as a "clearly knowing" situation. However, when the content being informed or prompted is ambiguous, we cannot assume that regulatory authorities have fulfilled their full disclosure obligations. In the case of Jin's assistance in information network criminal activities [11], Jin used his five bank cards to register an account and participate in buying and selling virtual

currency. Although his bank card was automatically stopped by the bank for three days during the transaction (the automatic stop payment mechanism refers to the automatic program mechanism that suspends transaction services when the bank detects abnormal fund flow direction of the bank card), the bank card stop payment is automatically released after three days. This means that although each bank card has shown automatic stop payment situations one after another, transmitting signals of abnormal fund flow of the bank card, Jin has not received clear notification from beginning to end. He is unaware that the five bank cards have been used for fraudulent fund transfer, and he is aware of the situation. At most, it is possible that there is an unknown flow of funds in one's own bank card, and one cannot have a considerable understanding of the possibility that his own buying and selling of virtual currency can greatly help with cybercrime activities. Therefore, it should be recognized that Jin is not a "should have known" situation. On the contrary, he has a relatively low educational background, and has limited knowledge and legal awareness of related cybercrime situations, From his perspective, the automatic suspension of five bank cards by the bank is not enough to alert him to criminal situations, let alone the subjective intention of providing assistance. Similarly, in observing the case of Xing helping with information network criminal activities [12], when he applied for a bank card, he personally signed the "Notice on Suspected Illegal Activities in Selling, Lending, Renting Mobile Cards, Bank Cards, Identity Documents, Corporate Accounts, etc.", indicating that he was clearly informed by relevant personnel that providing bank card and other payment settlement services for online criminal activities is a crime of assisting trust. Xing himself has been fully and effectively informed of the relevant legal provisions, so it can be determined that Xing's subsequent provision of seven bank cards for fund transfer is an act of actively providing assistance for online crimes. Xing constitutes a constituent element of "clearly knowing" and is clearly "should have known". Type.

Based on three cases, we believe that when determining whether the person providing assistance can recognize the legal infringement of their own assistance behavior, attention should be paid to the clarity of the information received by the person providing assistance. The requirement for "clarity" of this information is not simply to impose a short-term ban on the account without explanation, but rather to examine whether the information obtained by the perpetrator when informed can clearly indicate that the perpetrator is in a "knowing possible" state. In other words, the perpetrator only knows that the behavior they are carrying out will most likely be used to assist in criminal activities. If the perpetrator still insists on carrying out the behavior or allows a certain kind of assistance situation to exist, then we can determine that the perpetrator is in a "should have known" state, and at this point, he constitutes the subjective element of "clearly knowing".

4.2 In Third-party Platform Provision or Server Subletting, the Provider or Sublessor Should be Deemed as "Clearly Knowing"

Individuals, units, or organizations that provide third-party platforms or server subleases can achieve comprehensive and real-time monitoring of the usage behavior of

server tenants due to existing server technology. The author advocates that in such situations, the sublessor should be deemed to be in a "clearly knowing" state. The sublessor should have a clear understanding that their business activities may be used for cybercrime, that is, they should have a more cautious attitude and necessary preventive measures towards possible cybercrime situations. In the crime of Zhejiang T Company and Chen Moumou's helping information network criminal activities [13], T Company, as a unit providing a third-party platform for Internet advertising, failed to further identify the relevant background when facing advertisers who may be suspected of gambling, failed to perform regulatory obligations, and was found by the court to be applicable to the crime of helping trust. In the case of Chen's assistance in information network criminal activities [14], Chen sublet his server to gambling gang members for the circulation of online gambling funds. When Chen sublet the server, he contacted the criminals and should have had some understanding of the purpose of the sublet server. He used the reason that there was no need to know the operation content of the server after the transaction was completed to prove that he was not aware of the situation and thus proved that he was not responsible, which was actually an act of evading regulatory obligations. For the platform provider of the server itself, there is a certain regulatory obligation for the operation or activities of its own server, and it also has a considerable regulatory obligation for the sublet server. In other words, for the sublessor, as the tenant of the original server, they should be aware that renting a server cannot be used for related cybercrime activities. When carrying out subletting activities, they should be vigilant about possible cybercrime assistance activities. For platform providers or server sublessors, they should have a clearer understanding and assessment of potential cybercrime risks in their business operations.

5 Judicial Inspiration and Suggestions

5.1 Judicial Inspiration

The criteria for criminalizing the crime of assisting information network criminal activities are still relatively vague, with the possibility of improperly expanding the scope of punishment. Its characteristics include vague extension of the charge, generalization of objective behavior patterns, and lower statutory penalties. The author starts from the key constituent elements of the crime of "clearly knowing" and believes that its meaning should include "clearly knowing and should have known" (the latter refers to the situation where a presumption of knowledge is made in the context of existing basic facts and evidence chains), and the boundary of "clearly knowing" should be further limited and explained. In the experience of judicial cases in China, two standards should be summarized to further clarify the specific circumstances of "presumed knowledge". Therefore, in the judicial judgment of the crime of assisting information network criminal activities, the core issue of determining the charges will be clearer in the relevant provisions or provisions, and the reasoning and inference in each specific situation will be more fair and objective. Therefore, the author further believes that regardless of whether a non prosecution opinion or judicial judgment is made, it is necessary to form a complete logical chain of relevant evidence that is

clearly recognized, combine academic theory with judicial practice, establish more direct reference standards, so as to better play the role of fallback clauses and reduce the consumption of judicial resources during the trial of such cases.

5.2 Policy Recommendations

Based on the above judicial experience and article analysis, we propose the following suggestions:

Relevant departments should raise the threshold for disclosure obligations and effectively fulfill relevant disclosure obligations, including warning obligations. For example, when the automatic stop payment program in the banking system is triggered, relevant information on the flow of funds from the bank card should be gathered to remind the perpetrator of the relevant risks. If there is a possibility that the neutral business behavior of the relevant regulatory authorities may be used to assist in cybercrime, then when there is a legal risk that the perpetrator should be reminded of, the notification procedure should be improved. For example, in the WeChat account unblocking account mentioned above, when WeChat unblocks the banned account, it clearly reminds the unblocker that it may be suspected of online fraud. In the author's opinion, in the process of judging knowledge, we should consider the scope of cognitive obligations of ordinary people in the context of the current Internet development or information technology iteration, so as to better define neutral business behavior, and at the same time ensure that people's reasonable freedom of life is not damaged by excessive criminal law requirements.

Due to the ease of utilizing third-party online platforms and server rental services in cybercrime activities, we advocate for the expansion of regulatory obligations for service providers and sublessors, while referring to their professional background and business experience as a reference. As practitioners or relevant stakeholders, their awareness of potential risks in helping cybercrime activities should be higher than that of the general public. This also means that market regulation needs to improve relevant provisions, further clarify the obligations that the aforementioned parties should bear in transactions, and promote the healthy development of the server rental market under regulation.

6 Conclusion

In the analysis of this article, vivid judicial cases and document analysis are the ultimate source of the author's viewpoint. After extracting the standards or references for judgments, it returns to the level of academic theory and serves as a bridge between theory and practice. There is still a gap in research on platform server sublessors, as sublessors with corresponding knowledge background and information technology capabilities have the ability to understand the service content provided by the platform. However, is the threshold for such knowledge background and corresponding capabilities relatively low for ordinary people? If it is assumed that sublessors should have corresponding capabilities and assume relevant obligations in judgment cases, is

it conducive to cracking down on the crime of assisting information network criminal activities? I will conduct further research here in the future.

References

1. Anna Urbanovics, Cybersecurity Policy-Related Developments in Latin America, 21 AARMS 79, 79 (2022), https://doi.org/10.32565/aarms.2022.1.6.
2. E. R. Fissel & J. R. Lee, The Cybercrime Illusion: Examining the Impact of Cybercrime Misbeliefs on Perceptions of Cybercrime Seriousness, 56 Journal of Criminology 150, 150 (2023), https://doi.org/10.1177/26338076231174639.
3. Yu Haisong. Judicial Limitations and Specific Implementation of the Crime of Assisting Information Network Crime [J]. Journal of the National Institute of Prosecutors, 2022, 30 (06): 101-113
4. Li Hong. On the Nature and Application of the Crime of Assisting Information Network Crime [J]. Legal Application, 2017, (21): 33-39
5. Yu Haisong. Judicial Limitations and Specific Implementation of the Crime of Assisting Information Network Crime [J]. Journal of the National Institute of Prosecutors, 2022, 30 (06): 101-113
6. Pi Yong, Huang Yan. On "Should Have Known" in Criminal Law and the Expansion of Criminal Law Boundary [J]. Chinese Prosecutor, 2012, (09): 76
7. Wang Shenghua, Zhang Xingxun. On the Judgment of "Clearly Knowing" in the Crime of Assisting Information Network Crime [J]. Journal of Jiangsu Police Academy, 2023,38 (06): 22-31
8. Liu Xianquan, Fang Huiying. Difficulties in determining the crime of assisting information network criminal activities [J]. People's Procuratorate, 2017, (19): 9-12
9. Wang Xiao, Cui Xinzhu. Identification of "Clearly Knowing" in the Crime of Assisting Information Network Criminal Activities [J]. Journal of Beijing University of Posts and Telecommunications (Social Science Edition), 2023,25 (06): 50-58. DOI: 10.19722/j.cnki.1008-7729.2023.0110
10. Case of Gao Dan and Others Assisting Information Network Criminal Activities, Criminal Judgment of Jianggan District People's Court in Hangzhou City, Zhejiang Province (2020) Zhe0104 Xingchu 413
11. Case of Jin Assisting Information Network Criminal Activities. The People's Procuratorate of Chaling County, Hunan Province [2022] Cha Jian Yi Bu Su Z1
12. Song Rui, Yu Jiayi, Li Tao. Judicial Application of "Clearly Knowing" in the Crime of Assisting Information Network Criminal Activities [J]. Chinese Prosecutor, 2023, (02): 67
13. Zhejiang T Company, Chen, and Others Assisting Information Network Criminal Activities. The Supreme People's Procuratorate Released the Fourth Batch of Five Typical Compliance Cases of Enterprises Involved in the Case (2023)
14. Chen's Assistance in Information Network Criminal Activities Case, People's Procuratorate of Shanggao County, Yichun City, Jiangxi Province, Shangjian Xing Bu Suo (2022) Z2.