

The Judicial Imposition of the “Knowing” Element in Cybercrime of Assisting in Information Transmission and the Reconstruction of Rules

Yingxin Zhang *

College of Humanities and Social Sciences, Harbin Engineering University, Harbin, China

* Corresponding Author Email: yiuoushi33@gmail.com

Abstract. With the development of the digital economy, the cybercrime of assisting information transmission (hereinafter referred to as “aiding crime”) has experienced an explosive growth, becoming a highly prevalent type of cybercrime. However, there are numerous difficulties in the judicial determination of the core constituent element “knowing” in this crime. In academia, there is disagreement over the determination of “knowing”, leading to three mainstream views: “clearly knowing”, “clearly knowing versus possibly knowing”, and “clearly knowing versus should know”. In judicial practice, issues arise such as inconsistent application standards, vague definitions in judicial interpretations, and difficulty in forming an evidence chain. Based on this, it should be clarified that “knowing” includes both “clearly knowing” and “should know”. At the same time, the rules for determining “knowing” should be reconstructed by improving laws and regulations, the boundaries of “comprehensive determination” should be delineated, and multiple perpetrators such as the perpetrator’s experience, the amount involved, and bank transactions should be comprehensively considered, persevering in the principle of unity between subjectivity and objectivity in the determination. For the perpetrators mentioned above, those with the most significant influence are given higher weights to establish the weight hierarchy among different perpetrators. This paper provides a reference for judicial authorities to standardize the application of the “aiding crime” to achieve a balance between crime and punishment.

Keywords: Aiding crime; knowing; judicial imposition; rule reconstructing.

1. Introduction

Nowadays, although social development has led to the vigorous growth of the digital economy, it has also given rise to new types of cybercrimes. In the era of the internet, the targets of crimes are computers or communication tools. The methods of committing crimes involve the extensive application of computer technology, presenting distinct characteristics such as strong concealment, wide dissemination range, and significant social harm [1]. Criminals, taking advantage of the information network technology in the digital economy, carry out acts that violate upon the legitimate interests of others, giving rise to the “aiding crime” offense. In 2023, courts nationwide concluded 102,000 cases of assisting in crime, indicates that this crime has become a prevalent offense in the field of cybercrime, showing an explosive growth trend and attracting widespread public attention [2]. Therefore, the academic community has conducted numerous discussions regarding the determination of “knowing” in the context of “aiding crime”. First, “knowing” is equivalent to “clearly knowing”, which is used to narrow the scope of punishment for this crime. Second, “knowing” should include “clearly knowing” and “possibly knowing”. As long as the perpetrator realizes the possibility that others are using the information network to commit crimes and still provides assistance, they can be included in the regulatory scope of this crime. Third, “knowing” should include “clearly knowing” and “should know”. It is suggested that specific determination scenarios should be delineated through judicial interpretations. The “Opinions on Issues Concerning the Handling of Criminal Cases Involving Assistance in Information-related Cybercrime Activities” (hereinafter referred to as the “Opinions on Assisting in Cybercrime”) has also made preliminary provisions on this matter. This opinion advocates persevering in the principle of consistency between subjective and objective aspects and making a comprehensive judgment based on the behavior of the

perpetrator, including their cognitive ability, transaction pattern, and profit situation. Meanwhile, at the level of judicial practice, there are diverse opinions on how to apply the aiding crime, especially the issue of “knowing” determination. Due to the blurry feature of the perpetrator's act, the judicial authorities have difficulty in determining whether the perpetrator had an intentional mindset and whether the objective act can meet the requirement of “knowing” in this crime. This situation can lead to inconsistent judgments in similar cases. Moreover, there are many irregularities in judicial application, and there are instances where ordinary online service behaviors are improperly classified as this crime [3]. For instance, in the case where Zhao Rui assisted in information network crimes, Zhao Rui registered a company to act as an agent for a third-party payment interface. Due to the interface being used for cybercrime, he was convicted of aiding crimes. This case demonstrates that neutral payment services have been wrongly criminalized. In this case, Zhao Rui's actions were those of a neutral technical service provided by a technician. There is no evidence to prove that he knew about the upstream crimes, but he was held accountable by the judicial authorities for the aiding crime. Therefore, focusing on the Judicial Imposition of the “knowing” Element and the Reconstruction of Rules in aiding crime, it is hoped that this will provide a reference for the current judicial authorities to standardize the application of the aiding crime.

2. The Judicial Imposition of the “Knowing” Element in Aiding Crime

2.1. Existing Theories have Inconsistencies in Their Determination of “Knowing”

Regarding the determination criteria for “knowing” in the aiding crime, there are mainly three mainstream academic viewpoints. First, some scholars maintain that “knowing” is equivalent to “clearly knowing”. They believe that the approach of “criminalizing through form and exempting through substance” should be adopted, and that the boundaries for the application of this crime should be determined by combining the restrictive feature of criminal law and the substantive penalizability [4,5]. Secondly, some scholars believe that “knowing” is equivalent to “clearly knowing” and “possibly knowing”. Believing that “possibly knowing” means that the perpetrator has doubts as to whether the person being helped has committed a cybercrime. Thirdly, the remaining scholars hold that “knowing” is equivalent to “clearly knowing” and “should know”. This is the mainstream academic viewpoint. It is believed that the principle of unity between subjective and objective aspects should be followed to infer that the perpetrator should have known. This approach can thereby control the judicial expansion of this crime and achieve a balance between crime and punishment [6]. The differences among these three theories have led to inconsistent judicial decisions in different regions, which have greatly influenced judicial credibility. Meanwhile, it will lead to fluctuations in the threshold for criminal charges, increase the difficulty of judicial practice standards, cause judicial personnel to lack clear, definite and unified standards for guidance when handling cases, and put the presumption of “knowing” in a dilemma.

2.2. In Judicial Practice, the Determination of “Knowing” in the Aiding Crime is Blurry

2.2.1. The application standards of judicial practice vary

The legal authorities of different jurisdictions do not have a uniform logic for determining “knowing”. Some judicial officers involved in case handling tend to fall into the trap of objective incrimination, believing that if a perpetrator engages in activities such as selling “two-card” devices or meeting the transaction volume requirements, they can be directly presumed to be aware of the situation [4]. Some investigators, however, insist that the probabilistic understanding standard should be taken into account. They require that the perpetrator must be able to prove that they have reached a high degree of certainty regarding the situation where others use the information network to commit crimes [7]. This difference directly leads to the situation where the same case is judged differently. For instance, when it comes to renting or selling bank cards to others for use, some judicial authorities hold that the act of renting or selling bank cards and the fact that some transaction amounts meet the

standard can be used to infer that the perpetrator had knowledge and thus be convicted. However, other judicial authorities believe that if the perpetrator can prove they were deceived, they can be determined to lack knowledge and thus not be considered guilty of a crime.

2.2.2. The rules defined in judicial interpretations are blurry

Compared with the “Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Networks and Assistance in Criminal Activities of Information Networks” issued by the Supreme People's Court and the Supreme People's Procuratorate in 2019, the newly released “Opinions on Assisting in Cybercrime” in 2025 more comprehensively stipulates the presumptive circumstances of “knowing”, places greater emphasis on the principle of consistency between subjective and objective aspects, and better aligns with the scenarios of new types of crimes. However, the “Opinions on Assisting in Cybercrime” still have blurry definitions for the circumstances of “knowing”. For instance, in the fifth article, “Based on the perpetrator's cognitive ability, occupation, past experience, relationship with the person being assisted, as well as their statements and defenses, etc., a comprehensive determination shall be made”, the term “comprehensive determination” does not clearly specify the extent of the comprehensive consideration, resulting in the inability of judicial authorities in the current practice to establish a unified standard.

2.2.3. It is difficult to establish a complete chain of evidence

The “knowing” in the aiding crime is mostly performed as indirect intent. Moreover, there are challenges in cybercrime investigations such as large amounts of data, easy to tampering, and cross-platform issues. There is no single tool that can obtain all the evidence at once; multiple methods need to be combined [8]. Under the current network technology, criminal activities are highly concealed and it is difficult to obtain direct evidence. The perpetrators often defend themselves by listing reasons such as “not knowing” or “being cheated”, and they can also destroy evidence by means of encrypted calls and deletion of records, thereby escaping investigation. The accomplices are also relatively concealed and difficult to discover, which made it impossible to obtain direct evidence such as documentary evidence or witness testimonies that could prove their knowledge [9]. However, there is no clear standard for the determination of indirect evidence of relevance. Although objective evidence such as bank statements, transaction records, and sales or rental activities are easy to obtain, it is difficult to prove that these evidence have a causal relationship with “knowing”. For instance, the perpetrator may have abnormal bank transaction records, but it is difficult to prove that they knew the money was being used for cybercrime. The development of network technology has given rise to new types of “helping in the crime” activities, leading to a problem where the formulation of laws fails to keep pace with social development. In these new types of “helping in the crime” activities, new methods such as virtual currency transactions have resulted in special forms of evidence. For instance, under existing mixcoin technology, methods like pooled funds mixing, random time delays, splitting transfer amounts, and not requiring users to complete real name authentication, make the forms of evidence quite special, significantly increasing the difficulty of obtaining evidence. The current laws and regulations do not clearly define the acceptance rules, which further increases the difficulty of proving “knowing”.

3. Reconstruction of the “Knowing” Rule in the Aiding Crime and the Guarantee Mechanism

3.1. “Knowing” Should be Equivalent to “Clearly Knowing” and “Should Know”

On the one hand, “knowing” should not include “possibly knowing”. “Possibly knowing” means that as long as the perpetrator is aware of the possibility of committing the helping behavior, it can be seemed as knowing the helping behavior. This would lead to an improper expansion of the legal application of the “aiding crime”, because the criteria for determining “possibly knowing” are blurry.

If it is included in the criminalization scope, it would result in “presumption of guilt in doubtful cases”, which violates the principle of legality of punishment. Moreover, the “Opinions on Assisting in Cybercrime” emphasizes the principle of consistency between the subjective and objective aspects and stresses the combination of subjective intent and objective behavior for determination. However, “possibly knowing” clearly lacks the support of objective behavior, which is inconsistent with the spirit of the judicial interpretation. Under the current trend of development of network technology, it is difficult for people to have a clear understanding of it. This is because network technology itself is inherently advanced and specialized, and it is unrealistic to expect ordinary people to have a grasp of it [10]. Therefore, if “possibly knowing” is included within the scope of “knowing”, it would put every ordinary person using network technology at risk of being convicted of the crime of aiding crimes. This is undoubtedly inconsistent with the principle of legality of crimes and punishments and would lead to improper application of the law in judicial practice.

On the other hand, “knowing” should be equated with “clearly knowing” and “should know”. Firstly, “clearly knowing” is definitely within the scope of “knowing”. If during the investigation by the judicial authorities, the perpetrator definitely express that they know that their actions are aiding in cybercrime, or there are other direct pieces of evidence that can conclusively prove that they clearly knew it is aiding in cybercrime, then this perpetrator undoubtedly constitutes the crime of aiding crime. Secondly, “knowing” should also include “should know”. Regarding this, the principle of consistency between subjective and objective aspects should be persevered. Although the perpetrator may not have definitely expressed “knowing” subjectively, through the perpetrator's subjective experience and the objective helping behavior, it can be determined that the perpetrator “should know”. On the objective side, it is necessary to distinguish the types of helping behaviors. On the subjective side, for network service providers and people with technical skills, the possibility of criminal liability for normal business activities should be excluded, and the excessive expansion interpretation of “possibly knowing” should also be further excluded [11]. At this point, it is necessary to emphasize the correlation between subjective and objective aspects. The cognitive ability of the perpetrator, previous experiences, the target of assistance, the profit situation, and other subjective and objective aspects should be comprehensively evaluated. At present, digital crimes exhibit the characteristics of “interconnection between online and offline” and “human-machine collaboration”. The perpetrators may participate in crimes through non-contact methods such as social media and encrypted communication tools [12]. This means that in the case of “knowing” in the crime of aiding crimes, the objective determination of “knowing” needs to take into account the cognitive characteristics in digital scenarios. For instance, in the case of “Yang Meilei's involvement in information network criminal activities”, Yang Meilei, despite knowing that the loan channels were illegal and the personnel handling the loans were unreliable, still went across provinces to make new mobile phone numbers, business licenses and corporate accounts. During this period, he also accepted others' reimbursement for food and accommodation expenses and handed over the accounts and U-shields to other people for use. His account transactions amounted to 39.23 million yuan, and there was also a case involving the flow of fraudulent funds. These abnormal behaviors are sufficient to infer that he was aware that others were committing crimes through the information network. Therefore, he was ultimately convicted and punished for the crime of aiding crimes. Furthermore, it is necessary to clearly understand the boundary between “should know” and fault. The fundamental difference between the two lies in whether there is an act of “avoiding awareness”. Regarding the distinction between the two, it is believed that the risk of behavior should be evaluated based on the evidence actually possessed by the perpetrator, and at the same time, the boundary for accountability in criminal negligence should be defined. Whether there is accountability can be determined based on the risk awareness that the perpetrator himself possesses regarding the evidence at his disposal [13]. Therefore, in the determination of “should know” and fault in the crime of aiding crimes, it is necessary to persevere in the principle that “should know” is based on the behavior of the perpetrator having an awareness of avoiding risks or actively providing help, and to clearly distinguish it from negligent crimes.

3.2. Setting the Boundaries of “Comprehensive Determination”

The “Opinions on Assisting in Cybercrime” does not clearly define the concept of “comprehensive determination”. Therefore, the degree of “comprehensiveness” should be regulated. The determination should be based on the perpetrator's experience, the amount involved, the bank transaction records, etc. The principle of consistency between subjective and objective aspects should be persevered in. That is, subjective knowledge needs to be verified through objective actions, and objective circumstances need to make a judgement of the subjective cognitive ability. Objective criminalization should be strictly avoided. Factors such as previous criminal records and abuse of power, which are decisive for the determination of knowledge, should be given higher weight. Moreover, based on the correlation and strength of influence among the factors, core factors, auxiliary factors, and exclusion factors can be distinguished to clarify the proof strength hierarchy of different factors. The core factors should include the perpetrator's previous experiences, occupation, and the content of their actions, such as having been punished for related crimes; after being restricted by relevant institutions for selling or renting “two cards”, they engaged in similar behaviors again; having a “two-card” transaction record with the person being helped before, and this transaction has been investigated by judicial authorities and suspected of involving fraud; engaging in professional activities such as network technology development or network software operation, or having a background in related computer science, possessing a higher cognitive ability than the ordinary person regarding the content patterns of cybercrime; preparing unified statements in advance to respond to investigations, or deliberately destroying chat records, transfer records, and other evidence; to escape supervision, using specialized tools which are specifically used for network crimes. It is believed that the auxiliary factors should include the amount of the involved funds and the understanding of the relationship, such as bank account transactions exceeding 300,000 yuan and the funds being transferred in and out rapidly, concentratedly transferred in and separately transferred out, which is significantly inconsistent with the behaviorist's daily income and consumption level; the large amount of transactions occurred immediately after the account is first used, which should exceed 5 times the perpetrator's average monthly income in the past 12 months, and the source of the funds cannot be explained legally; knowing that the person being helped has a history of cybercrime, still providing assistance, etc. The factors to be excluded should include the following situations: There is sufficient evidence to prove that the perpetrator is cheated, and the verification process has fulfilled the reasonable verification obligations by checking the business license, business contract, etc. of the person being helped; The legitimate funds in the transaction amount account for a large proportion, and legal transaction evidence can be provided; Students are cheated to participate, and they don't gain any profit or gained very little profit, and the participation time is extremely short. During the identification process, auxiliary factors play a role of being appropriately combined with the core factors, thereby enhancing the probability of the identification being seemed as knowing. During the identification process, one should first examine whether there are any exclusion factors. If such factors exist, it significantly reduces the probability of the identification being seen as knowing.

4. Conclusion

In the context of aiding crimes, the judicial determination of “knowing” is a crucial link in balancing the fight against cybercrime and protecting citizens' rights and interests. The theoretical disputes, blurry application and evidence challenge it faces require precise breakthroughs through a combination of theory and practice. Clearly defining the reasonable boundaries of “knowing”, discarding the judicial expansion of “possibly knowing”, and persevering to the principle of consistency of subjective and objective aspects are the core of regulating the judicial application of aiding crimes. By further refining and improving the laws and regulations, people can not only solve the problems of evidence collection and acceptance, but also unify the judicial determination criteria, effectively preventing the phenomenon of different judgments for the same case. Only by continuously improving the “knowing” determination rules and guarantee mechanisms can people

precisely hit the aiding crime, curb the spread of cybercrime, and at the same time persevere to the principles of criminal law's restraint and the principle of legality of crimes and punishments, so as to build a judicial guarantee line for the healthy development of the digital economy. However, there is a lack of clear regulations for the recently emerged new types of facilitation of crime activities, such as virtual currency transactions and AI technology support. Due to their advanced technology and new conditions and procedures, the existing judicial interpretations and understanding of these activities are insufficient, making it difficult to effectively respond and resolve them.

References

- [1] Al-Khater W A, Al-Maadeed S, Ahmed A A, Sadiq A S, Khan M K. Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access*, 2020, 8: 137293-137311.
- [2] CNR News. Interpretation Record of the Work Reports of the Supreme People's Court and Supreme People's Procuratorate: As I Have Suggested Efficiently Handle Every Case with High Quality. 2024.
- [3] Gu J, Song S. The Nature and Restriction of the Crime of Helping Information Network Crime. 2022 8th International Conference on Humanities and Social Science Research (ICHSSR 2022), 2022: 2343-2347.
- [4] Liu Yanhong. The Trend of Judicial Expansion of the Crime of Assisting Information Network Criminal Activities and Its Substantive Limitation. *China Legal Review*, 2023, (3): 58-72.
- [5] Xing W. Analysis of Judicial Practice and Dilemma Optimization of "Two Cards" Crime of Assisting Information Cybercrime. *Law and Economy*, 2024, 3(8): 22-32.
- [6] Yan Erpeng. Legislative Interpretation and Judicial Correction of the Crime of Assisting Information Network Criminal Activities. *Legal Science (Journal of Northwest University of Political Science and Law)*, 2024, 42(5): 117-128.
- [7] Jiang Lu Yi. From the Perspective of Duality: Judicial Determination of Knowledge of the Fact in the Crime of Assisting Information Network Criminal Activities - Based on 1,082 Relevant Judgments as Research Samples. *Journal of Law*, 2025, 46(5): 73-93.
- [8] Horan C, Saiedian H. Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy*, 2021, 1(4): 580-596.
- [9] Zeng Lei. The Logical Judgment and Scope Limitation of Knowing in the Crime of Assisting Information Network Criminal Activities. *Journal of the People's Public Security University of China (Social Sciences Edition)*, 2023, 39(1): 59-66.
- [10] Huang Xianqing. Research on the Issue of the Transformation of the Crime of Assistance in Information Network Cybercrime into the Crime of Principal Offender. *Legal Application*, 2022, (7): 70-78.
- [11] Zhou Y. Research on the Crime of Helping Information Network Crime. *Law and Humanities*, 2025, 1(3): 22-30.
- [12] Di Nicola A. Towards digital organized crime and digital sociology of organized crime. *Trends in organized crime*, 2022: 1-20.
- [13] Greenberg A. Why criminal responsibility for negligence cannot be indirect. *The Cambridge Law Journal*, 2021, 80(3): 489-514.