

The Boundary of "Knowing" in the Crime of Assisting Information Network Criminal Activities

Ziou Liu *

School of Law, Haihua College, Liaoning Normal University, Zhuanghe, China

* Corresponding Author Email: yuanlufuzhou@gmail.com

Abstract. In recent years, the number of cases of aiding and abetting information network crimes (hereinafter referred to as "aiding and abetting crimes") has increased, the groups involved have gradually expanded, and criminal behavior has shown a trend of universalization. One of the core elements in the determination of the crime of aiding and abetting is the rule for determining knowledge in the crime of aiding and abetting. Nowadays, there is a problem of expanding the application of "presumed knowledge" in judicial practice. In addition, "knowledge" itself has complex characteristics such as indirectness, unidirectionality, and predictability, which makes it difficult to prove subjective elements and prone to the risk of objective attribution and "different judgments in the same case". This article points out that the reasonable definition of the boundary of "knowing" should be based on the principle of modesty in criminal law, strictly distinguishing between civil violations and criminal illegality, and through the introduction of typological situational judgment standards, combined with the specific cognitive abilities and behavioral scenarios of the perpetrator for evaluation, strictly regulating the application of criminal presumptions, clearly distinguishing between factual presumptions and legal presumptions, and fully safeguarding the defendant's right to refute, preventing the erroneous upgrade of "should know but did not know" to "knowing", and constructing a comprehensive identification system that unifies subjective and objective factors.

Keywords: Assisting and facilitating the use of information networks for criminal purposes; knowing; comprehensive determination.

1. Introduction

With the continuous development of information network technology and its deep integration into society, today's cybercrime is showing characteristics of chain and division of labor. In order to combat those who provide technical support or assistance for crimes, the Ninth Amendment to the Criminal Law has added the crime of aiding information network criminal activities (hereinafter referred to as the "aiding and abetting crime"). According to data from the China Judicial Big Data Research Institute, the number of cases of aiding and abetting crimes has shown an explosive growth trend from 2017 to 2021. The number of cases surged 34 times in 2020 and further increased 17 times in 2021. From this data, it can be seen that the behavior of aiding and abetting is showing a trend of "universalization", and the criminal behavior of aiding and abetting is spreading from professional technical fields to ordinary social groups (such as students). The generalization of the subject of the crime of aiding and abetting trust poses a serious challenge to the accurate determination of subjective elements in judicial practice. There is a core institutional issue in the current judicial determination of the crime of aiding and abetting, which is the generalization of the presumption of "knowing". This generalization is reflected in two levels.

One is the formation of a macro level pattern of "presumption as a principle and comprehensive recognition as an exception"[1]. The formation of this pattern is caused by multiple factors. Article 11 of the Interpretation of the Crime of Assisting with Trust, as a presumption rule, is easily misunderstood as the core principle of identification, which tends to directly deduce that the perpetrator has "knowledge" based on certain types of objective behavior, making it difficult to cover new types of online assistance behavior [2]. The provision of "other sufficient grounds for determining knowledge" in this article gives investigators too much discretion, promotes the generalization of presumption, and actually weakens the examination of the subjective state of the perpetrator; In addition, the requirement for "comprehensive identification" has long been limited to

"two card" cases, and this more cautious, detailed but time-consuming identification method often occupies a secondary position in the face of the high incidence and difficulty of proving information network crimes. This situation has led to an erroneous tendency in judicial practice of "presumption as the principle and comprehensive recognition as the exception".

The second issue is that at the micro level, it also causes the problem of "knowing" being easily expanded and explained. The ambiguity of the presumed basic facts and insufficient proof standards make the threshold for presumption too low, and the basic facts themselves are easily interpreted broadly, resulting in neutral assistance behavior being included in the criminal evaluation system; The ambiguity of the standard of proof can easily lead to a substantial shift in the burden of proof, partially shifting the responsibility of proving the subjective intention of the perpetrator that judicial personnel should bear to the perpetrator, lowering the evidentiary threshold for conviction. However, there is also a problem of excessive inclusiveness in comprehensive recognition, which leads to the expansion of the interpretation of "knowing". In practice, comprehensive recognition often relies on the personal experience of judicial personnel and has not formed a unified and verifiable evaluation standard. This results in the conclusion of comprehensive recognition having both determinacy and a certain degree of uncertainty.

These two aspects work together, leading to the subjective element of "knowing" being easily expanded and interpreted in practice. Therefore, how to scientifically and accurately define the boundary of "knowing" in the crime of aiding and believing has become a topic of theoretical value and practical significance. This article aims to sort out the theoretical origins and practical difficulties of the recognition of "knowing" and construct a comprehensive recognition standard.

2. Theoretical Controversies and Practical Dilemmas

The core subjective element for the crime of aiding information network criminal activities is "knowing", which refers to the subjective cognitive state of the perpetrator towards others using information networks to commit crimes. It has characteristics such as indirectness, unidirectionality, foresight, and generalization. Its determination should adhere to the principle of consistency between subjective and objective factors, with the objective behavior of the actor as the core basis, combined with subjective and objective factors such as cognitive ability, past experience, transaction situation, and profit situation to make a comprehensive judgment. Specific and clear cognition should not be required, and excessive relaxation of the determination criteria should be avoided, which may lead to generalized criminalization.

2.1. Theoretical Genealogy of the Connotation of "Knowing"

On a theoretical level, "knowledge" can be distinguished as "deterministic knowledge" and "generalized knowledge".

Deterministic knowledge has a clear cognitive form, which refers to the perpetrator's clear and specific knowledge that others are using information networks to commit a specific crime, not only knowing the type of crime being assisted, but may even know important information such as specific means and goals. Characterized by specificity and clarity, as well as obvious subjective intent.

General knowledge refers to the fact that the perpetrator is not aware of the specific content and nature of the upstream crime but recognizes that the technical support or assistance they provide has a real possibility of being used by others to carry out criminal activities. In terms of cognitive level, general knowledge requires the ability to reasonably anticipate the risk of the assisted person engaging in illegal behavior based on specific circumstances and other factors, which is different from vague "possible knowledge" or simple, unfounded speculation.

One viewpoint (abstract epistemology) holds that it is only necessary to recognize that others may be committing some unspecified criminal act; Another viewpoint (specific understanding) holds that it is necessary to recognize the specific nature of the crime committed by the principal offender.

This theoretical divergence directly affects the criteria and methods for determining the subjective state of the perpetrator in judicial practice, leading to a tendency for some judgments to generalize their determination.

2.2. The Realistic Difficulty in the Determination of "Knowing"

The crime of aiding and abetting occurs in cyberspace, and it naturally has the characteristics of separating aiding behavior from upstream crimes, and the actors are not familiar with each other [3]. This leads to a scarcity of evidence that can directly prove the subjective "knowledge" of the perpetrator, and in practice, there may be a dilemma of losing key evidence, thus turning to indirect evidence and situational judgments. However, this path carries the risk of ignoring individual differences in one size fits all approaches and leaning towards objective blame.

Some viewpoints point out that there is a tendency in practice to inappropriately equate "inference" with "knowledge". But 'presumption' itself is only a logical reasoning method and fact-finding tool based on basic facts to deduce the facts to be proven (i.e. knowledge). If this reasoning conclusion is directly used as the final "knowledge" for criminalization, it will evolve into an analogy that is unfavorable to the defendant, which violates the principle of criminal law.

The expanded application of this presumption erodes the spirit of modesty in criminal law and puts the crime of aiding and abetting at risk of becoming 'pocket crime'. The application of this presumption still carries the risk of substantial transfer of burden of proof in the procedure [4]. That is to say, when the prosecution completes the preliminary presumption by listing the basic facts, the burden of proof shifts to the defendant. The defendant needs to provide evidence to prove that they "did not know", which is equivalent to requiring the defendant to prove a negative fact, which is extremely difficult in practice. In addition, there is a natural gap between the defendant's ability to collect evidence and that of prosecution, especially in the highly specialized field of network technology. Resulting in its legal right of rebuttal being difficult to obtain substantive protection in reality.

From the perspective of legal application, there is a problem of presumed knowledge of the expansion of application [5]. Many behaviors in real life that are considered as aiding and abetting are neutral business or daily life behaviors, that is, neutral helping behaviors. The criteria for judging neutral assistance behavior include the legitimacy of the behavior, based on whether the behavior has an independent and legitimate purpose, whether it complies with technical specifications and business practices; The second is the promoting effect on crime, based on whether the behavior directly assists the illegal act or amplifies the harmful consequences of the assisted illegal act; The third is whether the actor has fulfilled the duty of care, whether reasonable preventive measures have been taken by the actor, and at the same time, the principle of proportionality should be followed, and excessive obligations such as universal monitoring should not be required. If the perpetrator is held criminally responsible simply because the behavior is objectively used by others for criminal purposes, improperly expanding the scope of punishment will inevitably lead to the suppression of normal network innovation, commercial activities, and technological development. Distinguishing between punishable acts of assistance and non-punishable acts of neutral assistance is another key to defining the boundary of 'knowing'. This requires judicial officials to carefully consider factors such as social norms, business legitimacy, and the degree of promotion of the crime when determining "knowledge", in order to avoid subjective attribution due to the occurrence of objective results.

3. Defining the Boundaries of "Knowing"

3.1. Establishing a Comprehensive Recognition System Integrating Subjective and Objective Elements

In response to the problem of subjective and objective disconnection in the current recognition of "knowing", it is necessary to build a comprehensive recognition system that balances precise accountability and rights protection based on the modesty of criminal law. The basis for constructing

this system is the principle of modesty in criminal law. This requires a strict distinction at the subjective level between the "illegality awareness" required for civil and administrative violations and the "knowledge" required for criminal offenses in terms of the degree of accountability, in order to avoid directly elevating general and vague illegality awareness to "knowledge" for criminal accountability [6].

The core of building this system is to introduce typological contextual judgment criteria. That is to say, a single and rigid standard cannot be used to judge "knowing". It should be combined with specific behavioral scenarios and fully consider the individual factors of the actor, such as their cognitive level, professional experience, behavior style, and post event performance, for a comprehensive evaluation [7, 8].

By mutually verifying objective evidence with these subjective contextual factors, it is possible to accurately determine the true subjective cognition of the perpetrator and define the boundary of "knowing".

3.2. Strictly Regulating the Application of Criminal Presumption

For presumption methods that cannot be completely avoided, it should be ensured that their application complies with the principles of subsidiarity and modesty.

The auxiliary emphasis on presumption is only a supplementary means of evidence proof. When it is possible to prove "knowledge" through direct evidence or sufficient indirect evidence chain, priority should be given to using evidence to prove it.

Humility requires restraint in the application of presumption, and one of the key factors is that "knowing" is a subordinate concept of "should have known and already knew". Knowing "is a cognitive element of intentional crime, which requires the perpetrator to actually recognize the possibility of the crime; 'Should have known but did not know' is negligence, which only requires the perpetrator to know but not due to negligence. It can be distinguished by factors such as whether there is active avoidance behavior and whether the duty of care has been fulfilled. In judicial practice, "should know but not know" (i.e. negligence) should never be treated as "knowing" (intention), otherwise the boundary between intention and negligence will be confused, leading to judicial chaos of "different judgments for the same case"[9].

By clarifying the applicable conditions of presumption, such as the need for conclusive basic facts, logical reasoning process, and the establishment of a mechanism to safeguard counter evidence, such as clarifying the standard of proof for the defendant's counter evidence and allowing professional witnesses to testify, the problem of presumption abuse can be solved.

The application of norms should strictly distinguish between factual presumption and legal presumption. Fact presumption is based on known basic facts and logical reasoning to arrive at the conclusion that the facts to be proved exist. Legal presumption, on the other hand, has legal provisions. If the basic facts are established, the facts to be proved must be recognized as established. While strictly distinguishing between the two types of presumptions, it is also necessary to effectively safeguard the defendant's right to refute. The effectiveness of any presumption is preliminary and rebuttable, and the defendant's procedural right to present counter evidence, question basic facts or reasoning process must be guaranteed [10]. The ultimate establishment of the presumption should be based on the principle of "overturning without evidence to the contrary".

3.3. Defining the Reasonable Boundaries of Accountability

At the behavioral level, through a comprehensive judgment that combines subjective and objective factors, neutral acts of assistance that are objectively used for criminal purposes but the perpetrator does not have specific or general knowledge subjectively, and the behavior itself has business legitimacy, are excluded from the scope of punishment for the crime of aiding and abetting [11]. That is to say, the combination of "knowing" and behavioral neutrality can be judged. If the perpetrator knows that others are using neutral behavior to commit a crime, and the behavior exceeds the normal

scope of business, it can be recognized as the crime of aiding and abetting; Otherwise, it will be excluded from prosecution.

At the cognitive level, it is necessary to set a bottom line for "general knowledge". Although the perpetrator is not required to be aware of the specific charges and details of the upstream crime, their understanding cannot be infinitely abstract or baseless suspicion[12]. What should be recognized is the nature of 'others using information networks to commit crimes', rather than some completely uncertain' possibly negative thing '. That is to say, the knowledge content must have a considerable correlation with "criminal" activities, rather than general illegal or irregular behavior.

4. Conclusion

The determination of the element of "knowing" in the crime of information network crimes is the key to balancing the punishment of crimes with the protection of human rights and the maintenance of online order. This article first reveals the problem of generalization in the current recognition of "knowing", that is, at the macro level, a pattern of "presumption as a principle and comprehensive recognition as an exception" has been formed, and at the micro level, there are also problems of vague presumption based facts and insufficient proof standards leading to the generalization of the recognition of "knowing". In practice, due to the particularity of information network crime activities and their aiding behaviors, there are difficulties in collecting objective evidence, insufficient protection of the defendant's right to refute, and blurred boundaries for the criminalization of neutral aiding behaviors.

In response to the above issues, this article proposes a systematic solution path by constructing a comprehensive identification system that unifies subjectivity and objectivity, strictly regulating the application of criminal presumption, and defining reasonable boundaries for attribution to regulate the boundary of recognition of knowledge.

However, this study also has certain limitations. Firstly, the research is mainly based on normative documents and theoretical deduction, and the empirical analysis and big data mining of a large number of cases are still insufficient, failing to fully reveal the subtle differences in specific discretion in different scenarios. Secondly, for the technical elements in the determination of "knowing", such as algorithm recommendations. There is still room for further elaboration on how to influence subjective cognitive judgments. In addition, the solutions focus more on the judicial determination process, and there is relatively limited exploration on how to reduce disputes from the source, that is, from the management and administrative supervision of network service providers.

With the iteration of new forms of cybercrime, such as the use of metaverse and deepfakes, criminal assistance will become more covert and technical, posing unprecedented challenges to the proof of subjective knowledge. Future research should pay more attention to interdisciplinary perspectives and deepen empirical research to achieve the best balance between combating crime, safeguarding human rights, and maintaining online order.

References

- [1] Wu Hongqi. Normative review and generalized correction of the recognition rules for the crime of aiding and abetting. *Legal Forum*, 2025, 40(2): 17-27.
- [2] 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.
- [3] Du M. Research on the Regulations of the Aiding Crime in China's Cybercrime Legislation. 2021 4th International Conference on Humanities Education and Social Sciences (ICHESS 2021), 2021: 2121-2125.
- [4] Wang Xing. Continuation of the Criminal Procedure Law on the presumption of proof of knowledge. *Contemporary Law*, 2025, 39(4): 100-113.
- [5] Long Zongzhi, Hu Jia. The determination of knowingly aiding in the crime of information network crime. *Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition)*, 2024, 45(1): 61-72.

- [6] Dan Jia, Liang Teng Tang. Misunderstandings and rectification in the judicial application of the crime of aiding information network crimes. *Nanhai Law*, 2024, 8(3): 43-54.
- [7] Cheng H, Li P, Li S. Definition of Knowing of Internet Service Providers in Helping Cybercrime. 2022 6th International Seminar on Education, Management and Social Sciences (ISEMSS 2022), 2022: 3645-3655.
- [8] Cai X, Deng J, Yan X. On the Types and Cognizance of Knowing in the Crime of Aiding Information Network Crime. 2022 8th International Conference on Humanities and Social Science Research (ICHSSR 2022), 2022: 2096-2101.
- [9] Zhang Jicheng. Interpretation of the Legal Logic of Knowing, Should Know, Knowing and Their Related Concepts. *Law*, 2023, (6): 20-33.
- [10] Sun Yuan, Liu Huihui. The negation of criminal legal presumption and the essence of permissible presumption. *Jiao Tong University Law*, 2025, (1): 5-21.
- [11] Schwemer S F, Mahler T, Styri H. Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act? *Oslo Law Review*, 2021, 8(1): 4-29.
- [12] Lu Jie, Yan Erpeng. Assisting in the Establishment, Positioning, and Identification of the Crime of Information Network Crime: Empirical, Theoretical, and Rule Based on 26 Criminal Second Instance Correction Judgments. *Journal of Criminal Law*, 2023, 75(3): 1-26.