Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.34006

Assistance in Determining "Knowledge" and Its Application in the Crime of Information Network Criminal Activities from the Perspective of Criminalization

Jiayi Lu

School of Politics and Law, Hubei University of Arts and Science, Xiangyang, China
xie52013142026@outlook.com

Abstract. The Ninth Amendment to the Criminal Law criminalizes the act of assisting in information network crimes independently, establishing the legislative model of making the offense of assisting in information network crimes a principal offense. "Knowledge" is the core of the subjective constituent elements of the offense of assisting in information network crimes, and its coverage and identification criteria directly determine the boundaries between crime and non-crime, as well as between this crime and that crime. Currently, there are core dilemmas in the identification of "knowledge" such as ambiguity in connotation, disagreement in object, abuse of presumption, and lack of hierarchy. This article clearly divides "knowledge" into three major types: explicit knowledge, general knowledge, and presumed knowledge. At the same time, people should establish a three-tier application path for the restriction and induction of "knowledge" in a hierarchical manner, which includes "clearly presuming whether the basis for its determination is comprehensive, strictly limiting the application of catch-all clauses, and improving the mechanism for identifying counterevidence". This reasonable approach not only aims to strike a balance between combating cybercrime and protecting legitimate network services but also achieves the final goal of adapting criminal responsibility to punishment.

Keywords: Assisting in the crime of information network activities, knowledge, principal offender

1. Introduction

With the rapid advent of the digital era, information networks have become a core driving force for promoting rapid economic development, facilitating people's lives, and promoting social harmony and progress. In November 2015, the Ninth Amendment to the Criminal Law of the People's Republic of China added the crime of assisting in information network crimes, making the act of assisting in a variety of information network crimes a separate crime. Scholars have also provided relevant practices and discussions to some extent, suggesting that the crime of assisting in information network crimes should be viewed from the perspective of the principal offender [1]. However, at the same time, the iterative upgrading of technology has also lowered the threshold for the emergence of cybercrime, accelerating the shift of various traditional crimes to cyberspace.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.34006

The traditional mainstream view holds that the criminalization of online assistance behavior is based on the independent criminalization of assistance behavior, which is independently punishable and no longer dependent on the principal offender. It requires a one-to-one corresponding subordinate relationship between assistance behavior and assisted criminal behavior. Given the high incidence, frequent occurrence, and diverse trends of information network crimes, it is often difficult to accurately distinguish them in practical application, necessitating some degree of restriction [2]. Among them, assisting in information network criminal activities, as an important link in the network crime industry chain, has become a "hotbed" for breeding various types of network black industries and facilitating the spread of crimes. In spite of the successive issuance of judicial interpretations and guidance opinions by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security of the People's Republic of China, clarifying the standards for conviction and sentencing, as well as the rules for legal application of this crime, gradually addressing various issues such as inconsistent standards in judicial practice. However, in the face of emerging new types of assisting behaviors, and how to precisely grasp the constitutive elements of crimes, clarify the boundaries between crimes and non-crimes, people work out keys between this crime and that crime, and punish the actual perpetrator of the crime according to law while achieving a positive unity of legal and social effects, remaining an important issue facing theoretical research and judicial practice [3].

Based on this, this article focuses on the identification and application of the crime of assisting in information network criminal activities from the perspective of the principal offender. By utilizing comparative research methods, it delves into the connotation of "knowledge" regarding its relevant legal application and identification standards. It also examines the controversies surrounding some aspects whether it includes "constructive knowledge", whether explicit knowledge of specific crime is required, and the boundaries of general intent, considering the prominent issues and development trends of this type of crime. This analysis delves into the challenges of the "knowledge" issue in current judicial practice. It not only aims to understand the mindset and reasonable expectations of both parties involved in judicial practice, but refines the approach to narrowing the scope of the "knowledge" issue, providing effective references for combating the crime of assisting in information network criminal activities, improving the governance system of cybercrime, and strengthening the digital security defense line [4].

2. Discussion on the typological meaning of "knowledge"

Regarding the types of "knowledge" in law, discussions involve concepts such as "actual knowledge", "constructive knowledge", "possessive knowledge", and "potential knowledge". However, in current criminal legal provisions, only the type of "actual knowledge" has gradually appeared in these years. Previously, the prevailing practice in Chinese judicial practice was to interpret "actual knowledge" as either "should have known" or "knew", here, "know" is essentially equivalent to "certain knowledge", which is the narrowest sense of "express knowledge". This interpretation restricts the meaning of "know" from its literal sense. In order to determine the type of knowledge possessed by the parties involved in the case, another approach is to make reasonable speculation on the subjective element of "should know" based on the specific type of case. However, it is always difficult to distinguish whether the parties are in a state of "potential knowledge" or "actual knowledge", and it is also challenging to determine whether they are aware of the potential infringement of their legal interests [5, 6].

This article discusses whether "should know", "known", or "or know" should be added to "knowledge", and the basis for this judgment is as follows. Firstly, whether there are difficulties in

DOI: 10.54254/2753-7048/2026.34006

obtaining evidence for the "knowledge" element in the evidence collection process. Secondly, whether there are many omissions in the punishment based on the "knowledge" element. From the perspective of the overall scope of the offense of assisting in information fraud, the objective constitutive elements of the act itself are relatively neutral in terms of language, the scope of punishment itself possesses a relatively broad nature, necessitating appropriate restriction on subjective elements. This is expected to maintain the stability of the punishment structure, ensure its effective judicial implementation in every practice, and enhance public trust and satisfaction with the judiciary [7].

"Knowledge" in the crime of assisting in information network criminal activities pertains to systematic abstract cognition, encompassing "clear knowledge" and "presumed ought to know", but excludes "pure speculation" or "possibility unsupported by any substantial evidence". The core of the matter is: it is sufficient to recognize the element of "using information networks to commit crimes" by others, without the need to explicitly know the specific charges, specific behaviors, victims, or the amount of money involved in the crime. An error in understanding the type of crime does not affect the establishment of "knowledge" [8].

Based on the research from the perspective of principal offender and various judicial practices, it can be summarized into three levels: The first level is clear knowledge. The perpetrator is fully aware of the specific type of crime, criminal means, criminal tools, criminal targets, surrounding environment, degree of harm, and legal consequences committed by others using information networks, as well as the specific role of their own assistance in this case. They possess a strong subjective malice, and their actions are highly harmful. At the second level, it is known as general awareness. Although the perpetrator is aware of others using information networks to commit crimes, they are not clear about the specific type of crime, the amount involved, or the consequences of the crime. They only have a certain general awareness of the illegality of their own assisting behavior. The subjective maliciousness and harmfulness of their behavior are moderate, so their punishment should be moderate. At the third level, constructive knowledge is presumed. The perpetrator may not have explicitly known the intention of others to commit cybercrime, but based on objective facts, it is presumed that to a certain extent, he should have known or had an obligation to know about his incriminating behavior. His subjective malice and the harmfulness of his behavior are relatively weaker, so his punishment can be mitigated. The incrimination paths for the above three situations should be differentiated, otherwise, their credibility and accuracy will be weakened in practical application, affecting judicial effectiveness [9, 10].

3. Identification of "knowledge" and its practical dilemmas

Based on the above content, the focus of the determination of "knowledge" is concentrated on two points. The first question is whether "knowledge" only means "clearly knowing" and whether punishment is only imposed based on this type in practice. The second question is which of "may know" and "should know" is a more reasonable criterion for determining "knowledge", and which is more likely to ensure fair trial of cases in accordance with the law. However, regardless of the type or degree of the dispute over "knowledge", the focus of the dispute lies in the contradiction between the effective punishment of the crime of assisting information network criminal activities and its disorderly expansion. It is suggested to further narrow the scope of "knowledge" based on the principle of reliance, standardizing it, and improving the applicable status of its identification and classification [11].

The dilemma in determining "knowledge" is summarized and concluded in the following three parts through extensive induction and analysis [12]. Firstly, the ambiguity in connotation. In judicial

DOI: 10.54254/2753-7048/2026.34006

practice, "should have known," "might have known," and "negligently unaware" are all encompassed under the term "knowledge," which blurs the distinction between intent and negligence, leading to an expansion of criminalization. In this context, the criteria for determining "knowledge" are unclear and its application is ambiguous, which can easily lead to misjudgments and wrongful convictions. This greatly increases the difficulty of implementing fair justice, leaving judges without a solid basis when encountering such legal cases. To a certain extent, it enhances the discretionary power of judges, thereby significantly increasing the practical risks of justice in such cases. Secondly, there are some differences in the objects of the crime. Some judgments require knowledge of the specific crime and specific means, while others only require knowledge of "the crime itself". The discretionary standards vary, making it difficult for the issue to be handled legally and reasonably by public authority within a certain scope, which increases the difficulty of judicial practice. Thirdly, the presumption of "knowledge" based solely on single facts such as "high profits, selling bank cards, and not knowing the other party" is prone to the dilemma of objective imputation, which restricts the implementation of judicial practice. In this case, the types and degrees of punishment show a tendency towards differentiation and are not standardized, which to some extent greatly reduces the credibility of justice and the public's trust in the law [4]. In summary, the determination of "knowledge" needs to be dramatically narrowed down and applied after reasonable restriction. This not only enhances the legality and rationality of judges' decisions but also greatly increases the public's trust in the judiciary. Although improving the accuracy and rationality of the application of "knowledge", people can achieve the goal of better justice and live up to the reasonable expectations of the public.

4. The restrictive approach to "knowledge"

From the perspective of criminalization, the restriction on the determination of "knowledge" in the crime of assisting and abetting is an inevitable requirement for adhering to the legislative intent and principles of criminal law, and it is irreplaceably necessary. The core of the criminalization of assisting in the crime of information network infringement lies in cracking down on assisting behaviors in cybercrime that pose independent social harm, narrowing the scope of punishment to precisely define the boundaries, avoiding the inclusion of negligent cognition and vague possibility cognition in the category of "knowledge," and preventing this crime from becoming a "pocket crime.".

The following is a discussion on the one-to-one corresponding narrowing methods for different types of "knowledge". "Presumed knowledge" is an important means to address the difficulty in directly proving "knowledge" due to the concealment of cybercrime. Ultimately, its core lies in reasonably defining the scope of "presumed knowledge", standardizing the application process of combining it with specific cases, avoiding abuse, clarifying "knowledge", limiting to direct evidence, and do not make a determination without direct evidence. Summarize knowledge, limit to a high degree of probability, and exclude vague speculation and generally suspicious situations. Presume knowledge, must consider multiple facts comprehensively, and prohibit presumption based on a single fact. Further clarify the applicable standards in judicial procedures [13].

Firstly, it is necessary to clarify the comprehensiveness of the presumption basis. "Knowledge" cannot be presumed solely based on a single objective fact. It should be combined with objective facts such as the perpetrator's own cognitive ability, professional background, family status, upbringing environment, behavioral motivation, and whether they have fulfilled reasonable duty of care, comprehensively assess whether the extent of "knowledge" meets the "high degree of

DOI: 10.54254/2753-7048/2026.34006

probability of cognition", excluding situations of "possible knowledge" and "should have foreseen", to avoid the error of imputation caused by not considering reasonable circumstances [14].

Secondly, the application of catch-all clauses should be strictly restricted. For situations not listed in judicial interpretations, the phrase "other circumstances sufficient to determine the perpetrator's knowledge" cannot be applied arbitrarily. It must reach a level of cognition equivalent to or higher than the listed situations, and it requires discussion and explanation of the presumption reasons by the collegiate panel, Ensure the rationality and normativity of presumption, so as to avoid expanding the scope of "knowledge" and reduce the impact of legal expansion on practice.

Thirdly, improve the counter-evidence mechanism, clarify the scope of the burden of proof for the perpetrator to provide counterevidence, which does not need to meet the standard of excluding reasonable doubt. It is sufficient to provide preliminary evidence to prove the lack of "knowledge". Judicial authorities should conduct a comprehensive review of the counterevidence. If the counterevidence is established, the presumption of knowledge should be denied, and the perpetrator should be declared innocent or not be held criminally responsible according to law, ensuring the restraint of criminal law presumption and avoiding objective imputation.

5. Conclusion

From the perspective of criminalization, the reasonable determination of "knowledge" in the crime of assisting and abetting requires the construction of a complete system of "type classification + restricted application + rule guarantee": in terms of determination rules, it is necessary to clarify that the extent of "knowledge" is limited to intentional cognition, excluding negligence and vague possible cognition, There is no need to rely on specific details of the principal offense; in terms of sentencing adaptation, differentiated sentencing considerations should be established based on the subjective malice corresponding to different types of "knowledge", to achieve the principle of proportionality between crime, responsibility, and punishment; in terms of practical safeguards, it is necessary to take into account the protection of legitimate network services, and apply higher standards for determining "knowledge" to entities such as network service providers and payment platforms, to avoid undue expansion of the scope of crackdown.

The research value of this article lies in its grounding in the legislative essence of the formalization of the crime of assisting and abetting, breaking the inherent logic of "knowledge" determination from the traditional perspective of accomplice, clarifying the coverage boundaries and differentiated narrowing schemes of different types of "knowledge", and to a certain extent, addressing the pain point of confusion in the determination of "knowledge" in judicial practice, It not only provides an operable theoretical guidance for judicial authorities to accurately apply the crime of assisting and abetting information crimes and avoid the crime becoming a "pocket crime", but also provides practical support for cutting off the network crime industry chain, maintaining a clear cyberspace, and promoting the construction of the rule of law in cyberspace. However, this article is limited to not combining empirical case data and not conducting quantitative analysis on the standard of knowledge for different subjects, It does not involve cross-border and new technology scenarios. In the future, it should further refine the rules for determining knowledge in different industries and by different entities, strengthen the connection between execution and the application of the principle of trust, and its research objects do not involve the whole world, lacking universality. It is also expected to be supplemented and improved, in order to achieve long-term stability in the future situation of cybercrime. In the future, with the digital society continuing to deepen, the forms of information network crimes will become more concealed and complex, and the judicial application of the crime of assisting and abetting in illegal activities will still face new

DOI: 10.54254/2753-7048/2026.34006

challenges. Under the framework of formalizing the offense of assisting in the commission of a crime, the identification of "knowledge" needs to be further refined, standardized, and systematized. It is expected that subsequent legislation and judicial interpretations will clarify the connotative boundaries of "knowledge", unify presumption rules, and reasonably distinguish between criminal illegality and administrative violations. As well as between criminal assistance and neutral business conduct, people aim to achieve a dynamic balance between punishing crimes and safeguarding the healthy development of the digital economy, adhering to the principles of criminal law restraint and legality and providing more scientific and robust criminal law support for cyberspace governance in the future.

References

[1] Von List, F. (2000) Textbook of German Criminal Law. Translated by Xu, J.S., Law Press, Beijing, 374, 376.
[2] Xu, Y.N. (2024) Study on the Limiting Path of The Offence of Aiding Criminal Activities in The Information Network. International Journal of Social Science and Education Research, 7(2),
[3] Stratenwirt, Kuhlen (2006) General Theory of Criminal Law I - Theory of Crime. Translated by Yang, M., Beijing Law Press, Beijing.
[4] Xiang, C.X., Li, J.Y., Xiao, X.R. and Zhang, W. (2024) Empirical Research on the High Incidence of Crime of Assisting Information Network Criminal Activities in Telecommunication Fraud Cases Based on 26, 121 Judgment Documents. Science of Law Journal, 3(4), 31-40.
[5] Nishida, N. (2013) General Theory of Criminal Law. Translated by Wang, Z.W. and Liu, M.X., Law Press, Beijing, 334.
[6] Roksin, K. (2013) General Theory of German Criminal Law. Translated by Wang, S.Z., Law Press, Beijing, 101.
[7] Chen, X.L. (2022) The Principalization of Accomplices: From the Perspective of the Crime of Assisting in Cybercrime. Comparative Law Studies, (2), 44-58.
[8] Chen, H.B. (2022) Correcting the "pocket-sized" interpretation of the crime of assisting in information network crimes. Journal of Hunan University (Social Sciences Edition), 36(2), 127-135.
[9] Ouyang, B.Q. and Liu, M. (2022) Application methods of the crime of assisting in information network criminal activities: from prioritizing this crime to prioritizing accomplice. China Applied Law, (1), 107-121.
[10] Liu, Y.H. (2023) The judicial expansion trend and substantive restriction of the crime of assisting in information network criminal activities. China Legal Review, (3), 57-72.
[11] Lao, D.Y. (2025) Protecting legal interests in the crime of assisting information network criminal activities. Jurisprudence Forum, 40(2), 5-16.
[12] Wang, Y.Q. (2025) Research on the overlapping issues related to the crime of assisting in information network criminal activities. Law Forum, 40(2), 28-41.
[13] Zhang, M.K. (2024) Re-examination of the Crime of Assisting in Cybercrime. Law and Business Research, 41(1), 21-41.
[14] Hao, Z.W. (2025) The Judicial Dilemmas in Determining the "Constructive Knowledge" of the Crime of Assisting Information Network Criminal Activities and the Reconstruction of Relevant Rules. Exploring Science Academic Conference Series, 8, 34-42.