Proceedings of ICSPHS 2026 Symposium: Ethics, Law, and Psychology: Interdisciplinary Reconstruction of Humanities in Medicine
DOI: 10.54254/2753-7048/2026.ZJU32770

Reconstructing the Standard for Determining the "Knowledge"Element in the Crime of Assisting and Facilitating in the Context of Minor Offence Management

Haohan Hu

Henan University of Economics and Law, Zhengzhou, China
2938536295@qq.com

Abstract. Against the background of minor offence governance, the tendency toward overly wide application of assisting and facilitating criminal activities crime conflicts with its inner requirements. Because of presumption rules in judicial interpretations and case pressures, the judgment of the "knowledge" element has been excessively expanded; thus, this causes an overly simplified confirmation process of "knowledge," a heavier proof burden on defendants, and unclear definitions of the "manifestly abnormal" clause. Therefore, under the guidance of principles including precision in minor offence governance, balanced leniency and severity, and efficiency and fairness equilibrium, we put forward the following: reshaping the judgment's conceptual framework, building an all-round assessment model, and activating the "contrary evidence" rule. These measures will narrow the scope of criminal responsibility, hence matching the demands of the minor offence era.

Keywords: minor offence governance, aiding and abetting cybercrime, "knowledge" requirement, presumption rules

1. Introduction

With profound transformations in China's criminal structure and governance model, the nation has entered an era of minor offences. Relevant data indicates that minor offence cases now constitute over 80% of the total caseload [1]. As a quintessential minor offence, the crime of assisting information network criminal activities has experienced explosive growth in recent years, consistently ranking among the top three offences in terms of prosecution numbers for several consecutive years [2]. The "pocket offence" tendency in such crimes is mainly driven by the presumption rule for the "knowledge" element established in the 2019 Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving the Illegal Use of Information Networks and Assisting Information Network Criminal Activities issued by the Supreme People's Court and the Supreme People's Procuratorate [3]. This presumption has unduly lowered the threshold for criminal liability in assistance and accomplice offences, while the relevant provisions on rebuttal evidence have not exerted an effective restrictive function. As a result, the inherent tension between such application and the governance of minor offences has become increasingly prominent. Against this background, it is imperative to clarify the constitutive

© 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.ZJU32770

boundaries of the "knowledge" element and reasonably limit its scope of application. This paper examines the practical difficulties in identifying the "knowledge" element of the crime of assisting in criminal activities, re-examines the criteria for establishing this element from the perspective of minor offence governance, and further optimises the specific approaches to determining "knowledge." It aims to provide a theoretical reference for unifying the judgment standards of the "knowledge" element, advancing the governance of minor offences and the construction of the rule of law in China.

2. Current status and challenges in determining the "knowledge" element of the crime of assisting and facilitating criminal activities

Since the "knowledge" element of the crime of assisting and facilitating criminal activities relates to the actor's subjective mental state, which is inherently concealed and difficult to verify directly, it can only be inferred and determined through external objective conduct. Yet exclusive reliance on objective conduct makes it hard to conduct a quantitative assessment of the level of "knowledge." The intertwining of subjective and objective factors has thus given rise to considerable difficulties in the identification of "knowledge" in judicial practice.

2.1. Over-simplification of the "knowledge" determination process through presumption

Article 11 of the Interpretation sets forth presumptive rules for proving "knowledge" in offences of assisting cybercrime. Although such a mechanism owns its rationality aspect, it has also excessively carried out over-simplification toward the identification of "knowledge," thus causing a certain degree of inflexible situation in conviction affairs.

In practical operation, the identification work of the "knowledge" element relies completely on matching with the presumed circumstances that are set down in judicial interpretation. The reasons can be divided into three aspects. First, cybercrime investigation activities have inborn difficulty. Different from traditional crimes, cyber offences have the characteristics of wide influence scope, fast technological change speed, and purely digital-form evidence. For public security authority departments, even though they possess quite a lot of investigation resources, the collected evidence often still belongs to circumstantial evidence, and usually cannot reach the strict evidentiary standards that are required for conviction. Therefore, the use of presumption rules to lower the evidentiary threshold has become an unavoidable practical necessity matter. Secondly, the proving work of "knowledge" itself has inborn complexity. The establishment that other information networks are being utilized for criminal activities is a core element when judging complicity in information network-related crimes. However, the confirmation of the actor's subjective "knowledge" is extremely difficult to carry out. In practical operation, such kind of knowledge is often determined according to the suspect's statement content. Driven by the instinct of pursuing profit and evading punishment [4], suspects frequently carry out fact distortion to hide the truth situation, even denying that they have awareness of others' criminal acts. This situation blocks the presentation of evidence, so the introduction of presumption rules is of crucial importance to break through the deadlock and push forward the proceeding process. Third, the combat against information network accomplice crimes is of urgent nature. Such crimes have large scale, deep harmful degree, and their methodology is constantly developing and changing. The appearance of new criminal technologies makes prevention work especially difficult, so timely and effective punishment is needed. The presumption rule can exactly meet this kind of practical need.

DOI: 10.54254/2753-7048/2026.ZJU32770

Thus, judicial practice usually makes determination procedures more simplified, putting case efficiency into prior position more than thoroughness, which causes rulings with excessive mechanization. The subjective "knowledge" demand is strictly limited inside the seven situations made clear in Article 11 ; thus, if any single condition is satisfied, it will establish a presumption of knowledge. This "objective liability" pattern seriously breaks the criminal responsibility principle which asks for the unity of subjective intent and objective conduct, and it may make innocent persons face unfair criminal accusations. Although presumption rules can raise short-term efficiency in dealing with accessory cases, their long-term use not only creates judicial distortions where "small fish are caught while big fish escape," but also makes investigation work lazy and increases over-reliance on guesses. Therefore, this twists truth-seeking, weakens judicial credibility, and is opposite to the basic goal of the criminal justice system that pursues fairness and justice.

2.2. The improper enhancement of the defendant's burden of proof

In judicial practice, the qualifying clause "unless there is contrary evidence" has practically become invalid in effect. Therefore, this improper transfer of the burden of proof to the defendant not thus conforms not to the criminal proceeding principle that the prosecution generally undertakes the burden of proof, that the defendant bears no obligation to prove his or her innocence to the court, and hence that the court must not make an adverse inference against the defendant based on this situation; furthermore, it also has the risk to turn presumptions into direct fact-findings [5]. During investigations, public security organs inherently neglect the collection of contrary evidence; furthermore, amid the state's intensive crackdown on telecommunications fraud, these authorities face substantial obstacles in investigating or verifying evidence that could rebut the presumptive conclusions. Under the heavy pressure of case adjudication, judges struggle to meticulously assessing on a case-by-case basis, whether an accomplice in telecommunications fraud "knew" or the extent of such knowledge. Therefore, they are compelled to conduct formal verification based on interpretation. Specifically, when an objectively corresponding act exists, that act is directly regarded as "knowledge." In all other circumstances, pursuant to Article 11(3) of the Interpretation, anomalous conduct is classified and "knowledge" is inferred accordingly.

This not allowable transfer of proof burden not only brings about a serious unbalance in defendant's proof responsibility but also dangers making suspects fall into a hard position where they cannot prove they are not guilty. At the same time, it damages the definiteness of legality principle and the protective functions of innocence presumption. On one side, legality principle requests to clearly define crime's constituent factors to guarantee predictability [6]. However, in cases related to information network crime supporting behaviors, the possibility of legal argument on subjective factors is removed, which makes the legal boundary of "knowledge" requirement unclear. Citizens feel hard to predict situations where evidence bad for them may be used, thus violating legality principle. On the other side, the use of innocence presumption has a precondition that all evidence collection methods have been used up; when evidence does not reach the true and sufficient standard, and there exists reasonable doubt on the facts supporting accusation, a judgment beneficial to defendant should be made. However, because criminal limitation clauses have no effect and the evidence strength gap between prosecution and defense is extremely large, the application of innocence presumption has become practically not possible.

DOI: 10.54254/2753-7048/2026.ZJU32770

2.3. Ambiguous definition of the "manifestly abnormal" element

Among related court documents, Article 11(3) – "where the transaction price or method is manifestly abnormal" – shows the highest utilization rate in "cognizance" determination, which takes up nearly half of all cases. This rule, having ambiguity and allowing wide explanation in both legislative and judicial practice, therefore carries risks such as unjust judgment of innocent persons and inconsistent decisions in similar cases.

While it was designed for wide application from the beginning, it does not have clear definitions for limiting clauses or subjective terms like "manifestly abnormal." For example, in common "two-card" crime cases, some persons hold that 2,000 yuan per set is "manifestly abnormal," while other persons maintain that any payment form is "manifestly abnormal." [7] This legislative method includes three core considerations. First, it aims to build comprehensive rules. Given the natural difficulties in investigating, prosecuting, and arresting cybercriminals, and the necessity of criminal punishment, defining aiding and abetting as an independent crime guarantees comprehensive deterrence. Especially when investigation of primary cybercrimes is difficult, application of the information network support crime ensures all persons involved in cybercriminal acts bear criminal responsibility. Second, considering the fast development of cybercrime methods and the delay of legal revisions, this rule is deliberately written in flexible manner, granting judges large discretionary power when dealing with new criminal patterns. Third, considerations of legal effect and stability require flexible legislation. This prevents frequent revisions needed to deal with developing cybercrimes, hence stopping public feeling of random "overnight policy changes."

This expansion trend is closely connected to legislative design and is further strengthened in legal practice by three key factors. First, as we have mentioned before, legislators have given judges large discretionary power. In practice, this too-large discretionary power will inevitably make court decisions affected by uncontrollable variables—judges' personal subjective views, case handling ability, and even regional legal practices. The lack of quantifiable decision standards causes problems such as inconsistent rulings in similar cases. Second, the concept of "manifestly abnormal conduct" has become a tool to avoid the difficulties in proving "knowledge." Because proving subjective "knowledge" is complex and costly, "manifestly abnormal conduct" is a vague standard that only needs showing objective actions, making it an easier choice for judicial organs. This ambiguity has led to over-use of "manifestly abnormal" instead of proving "knowledge." Thirdly, under pressure of too many cases compared with judicial resources, substantive evaluations have given way to formal examination. As time passes, judges have formed a fixed thinking: "manifestly abnormal → presumption of knowledge → conviction for aiding and abetting cybercrime."

3. The intrinsic requirements for determining the "knowledge" element in aiding and abetting the use of information networks under the context of minor offence governance

The basic principles and rules of minor offense control have inner connection with the core demands about the "knowledge" element which supports criminal acts in criminal offenses. Thus, when we think about minor offense control, redesigning the definition and practical use of this "knowledge" subjective element is not only logically suitable but also doable in legal practice.

Evaluating the "knowledge" element in accessory crimes needs detailed, unified, and specific rules. Based on the basic demand of foreseeability in criminal law, the minor offense theory came out to deal with public worries about the vagueness and unpredictability of criminal risks, limiting the randomness and over-expansion of criminal charges. As typical minor offenses, such crimes have hidden features, and common people often lack related legal knowledge. This makes ordinary

DOI: 10.54254/2753-7048/2026.ZJU32770

citizens very easy to get involved without knowing it, causing many marginal groups to face unfair criminal procedures. Furthermore, the current system for judging "knowledge" shows a very obvious expansion trend: its evaluation not only depends on the actor's subjective mental state but also is greatly affected by personal experience and free judgment of individual judges. This makes inconsistencies and judgment randomness in actual judicial practice even more serious.

Building the "knowledge" element in accomplice crimes needs a balanced method that combines leniency and strictness. This principle should spread through the whole chain of criminal legislation, judicial precedent, and law enforcement, becoming the core of the minor offense punishment system. In essence, this method puts first the differentiation of each case according to individual situations, making sure punishment matches the seriousness of the offense and providing forward-looking guidance for controlling accomplice crimes. This balanced criminal system decides the rule design about the "knowledge" element in two key aspects: Externally, because minor offenses have lower violence levels and relatively reduced social harm, complicity crimes need a lenient sentencing strategy—that is, "strict sentencing standards plus lenient decriminalization." Therefore, setting clear and strict standards for judging "knowledge" is very important: it stops the undue expansion of punishment scope while making sure that real criminal acts receive proper strict investigation and judgment. Internally, this single offense must be improved according to the subjective fault and different degrees of personal danger of the perpetrator. The depth and truthfulness of the perpetrator's "knowledge" act as key standards for differentiating penalties. By defining this originally unquantifiable subjective element through multi-dimensional evaluations based on objective external behaviors, judicial organs can carry out more accurate and targeted control and punishment for such crimes.

Similarly, the evaluation of the "knowing" element in the accessory offender also requires a careful balance between judicial efficiency and substantive justice. In the system of punishing petty crime, the criminal justice system should not give priority to the procedural economy at the expense of justice, but should strive to reconcile these two values. In terms of efficiency, its fundamental goal is to achieve maximum fairness and justice at the lowest judicial cost [8]. Specifically, raising the threshold for the establishment of "knowingly" in cybercrime accomplices can limit the scope of criminal conviction, reduce excessive workload, improve overall judicial efficiency, and achieve a more reasonable allocation of limited judicial resources. Criminal penalties should be completely excluded for acts that meet the objective constituent elements but have minor circumstances and negligible social harm [9].

4. Reconstructing the "knowledge" requirement for aiding and abetting cybercrime from a minor offence governance perspective

Guided by an analysis of the practical challenges in establishing the "knowledge" element and the theoretical principles of minor offence governance, refining the determination of this element not only better adapts to the era of minor offences but also enriches the theoretical foundation of the crime of assisting and facilitating criminal activities.

4.1. Reshaping the conceptual framework for determining the "knowing" element in the crime of assisting and facilitating

As philosophy precedes action, the key prerequisite for reconstructing the path to establishing the "knowledge" element from a minor offences governance perspective is to establish a new guiding concept, forming a restorative philosophy that "prioritises governance." Specifically, efforts should

DOI: 10.54254/2753-7048/2026.ZJU32770

focus on overcoming review inertia, shifting efficiency-oriented concepts, and eliminating policy interference.

At the front end, the assessment of the "knowledge" element must overcome the inertia of merely comparing cases against the seven scenarios outlined in Article 11 of the Interpretation. First, investigative authorities should conduct preliminary screening for three types of conduct: actions persisted in despite regulatory warnings; failure to fulfil statutory management duties after receiving reports; and frequent use of covert internet access, encrypted communications, data destruction, or false identities to evade supervision or circumvent investigations [10]. Given these behaviours are relatively objective, clearly defined and easy to assess, cases with no such unlawful conduct found after initial screening may proceed to subsequent evaluation.Second, examine cases involving the supply of criminal-specific programs, tools or technical support, [11] as well as technical assistance to help others evade supervision or obstruct investigations. These two conduct types are far harder to assess, as they overlap heavily with information-related crimes and legitimate daily activities. Identification relies heavily on context and subjective intent, often placing such acts in a grey area between lawful routine behaviour and unlawful activity.Despite this ambiguity, investigative authorities should adopt a comprehensive approach, considering the perpetrator's subjective stance to thoroughly review evidence and grounds for criminal liability, thus minimising unwarranted convictions. Finally, after reviewing the five specified conduct patterns, apply the catch-all provisions for transactions with obviously abnormal prices or methods, and other circumstances proving the perpetrator's knowledge. Notably, these catch-all provisions do not cover all conduct outside the five categories. They apply only when an individual's acts do not fit the five patterns but still require criminalisation under the law.

At the intermediate stage, public security and judicial organs must abandon the efficiency-first mindset when determining the "knowledge" element of the crime of assisting criminal activities, and avoid rushing investigations, prosecutions and judgments.To correct this, public security, procuratorial and judicial organs must cooperate closely while fulfilling their respective duties. Every step to verify "knowledge" requires extreme caution: public security authorities must fully collect and verify evidence; procuratorial organs should use non-prosecution safeguards to filter unqualified cases; judicial organs must adhere to criminalisation restraint. Thus, a three-tier review mechanism is formed to gradually narrow the scope of criminal responsibility. In addition, law enforcement and judicial personnel should focus on the long term rather than on short-term case completion rates. Appropriately narrowing the scope of criminalization can improve the long-term efficiency of justice, alleviate the backlog of cases, reduce the cost of error correction and stability maintenance, and improve the public's sense of security and judicial satisfaction.

In the final judicial stage, due to the exercise of independent judicial power by the people's court, the identification of "intentional" accomplices in cybercrime is not affected by the high-handed policy. However, in the context of frequent national campaigns and special actions against cybercrime (especially those focusing on SMS fraud), conventional judicial practice has been disrupted. Under political pressure, the judgment of accomplices often depends on unscientific assessment standards such as case acceptance rate and trial allocation quota. In order to reverse this situation, the people's court must adhere to judicial justice, adopt unified standards in the evaluation of "intentionality" requirements, and abolish unreasonable performance indicators formulated to meet political needs. This measure is crucial to prevent irrational indicators from leading to misjudgments that violate legal principles and the spirit of the rule of law.

DOI: 10.54254/2753-7048/2026.ZJU32770

4.2. Establishing a framework for determining the "knowledge" element based on comprehensive assessment

From a macro perspective, judicial practice must strictly adhere to the principle of comprehensive evaluation when identifying the "knowing" elements of the crime of helping information network crime. Statistics show that plea agreements and sentencing agreements apply to more than 90 % of such cases, greatly reducing the burden of proof to prove subjective knowledge. However, in cases where a few defendants refuse to plead guilty, the court should adopt a more rigorous and cautious approach to verify this subjective element. It is neither appropriate nor fair to rely on simplified presumption rules to reduce the standard of proof subjectivity. There is a significant risk of wrongful conviction in this way, especially when the defendant refuses to plea agreement or the factual relationship is in doubt. In this case, the application of the principle of comprehensive evaluation is not only appropriate, but also a necessary measure to maintain procedural justice and substantive fairness.

At the micro level, the comprehensive evaluation of "cognitive" elements should follow a fixed, step-by-step order to clarify the importance of evidence: first, examine the core cooperative behavior itself ; then, by supplementing the consideration of the defendant's personal background and plot, a well-structured and logically rigorous chain of evidence is constructed. First of all, the judge should comprehensively review the evidence directly related to cooperative behavior, such as transaction mode, payment channel, service consideration and so on. Such behavioral evidence often exists in electronic form, and there are major challenges in collection and verification, resulting in excessive reliance on suspects' confessions in cases. The court must be particularly vigilant about convictions based solely on statements, and must consider differences in the education level and cognitive ability of criminal suspects. Low education may lead to unstable or misleading statements, but some suspects may use this to disguise ignorance or lack of understanding. The judge should reveal the real subjective state through substantive fact review.

After evaluating the core behavioral evidence, the judge should comprehensively consider the overall cognitive ability and personal living environment of the criminal suspect. In view of the fact that individual background differences significantly affect the formation of criminal cognition, this paper proposes a hierarchical cognitive evaluation framework for individual variables. Judicial practice usually divides "cognition" into four levels: factual cognition, potential cognition, qualitative cognition and potential cognition. This hierarchical framework solves two practical problems : the high cognitive threshold of cybercrime and the lack of sufficient and clear foresight of most accomplices in the process of action. This also solves the problem of ambiguity in the definition of "understanding" of this crime. Specifically: practical understanding refers to the explicit and direct understanding of criminal behavior, which constitutes a complete subjective understanding. Probability cognition refers to the fact that criminal suspects realize that the probability of criminal behavior is extremely high, but due to the occurrence of future events, absolute certainty is unrealistic. This stage also constitutes an effective "cognition." However, due to the inherent substantive uncertainty of probability cognition, the presumption of guilt requires that probability cognition is not enough to establish criminal intent [12].

This phased framework particularly requires refinement regarding the most contentious category of "presumed cognition." This category essentially constitutes a legal presumption. Based on individual differences among suspects and contextual variations, this paper proposes the following criteria: First, for regulated industry entities and subjects bearing special statutory obligations (e.g., internet service providers), their professional responsibilities and industry-specific regulatory requirements may serve as grounds for recognizing the criminal efficacy of "presumed cognition."

DOI: 10.54254/2753-7048/2026.ZJU32770

However, for ordinary citizens, courts should prioritize judicial acceptability and apply the reasonable person standard: where conduct exceeds the cognitive capacity of an ordinary person, knowledge cannot be presumed. Conversely, if the danger meets this standard, suspects cannot claim ignorance as a defense. Second, regional economic and social disparities are critical: residents in economically developed areas with high cybercrime rates typically possess greater awareness of relevant complicity behaviors compared to those in less developed regions. Third, educational attainment correlates positively with cognitive awareness—higher-educated individuals demonstrate deeper understanding of illegal assistance activities. Crucially, tiered assessments based on personal backgrounds must adhere to comprehensive principles for holistic consideration. Adjudicators must avoid one-sided or superficial judgments based on a single factor alone, ensuring a holistic review of all relevant facts and circumstances to reach a fair and accurate determination of the "knowledge" element.

4.3. Activating the "contrary evidence" rule to restrain overly simplistic determinations of the "knowledge" element

The "contrary evidence principle" is a restrictive clause stipulated in Article 11 of the "Judicial Interpretation of Civil Litigation Evidence," which aims to restrain the excessive interpretation of the subjective element of "knowing." However, in the current judicial practice, this important safeguard measure has either been ignored or become a mere formality, failing to achieve the desired purpose. To activate its restrictive function, a three-stage framework is needed: to clarify the obligation of judicial notification, to reduce the burden of proof when the defendant submits rebuttal evidence, and to conduct a substantive review of all rebuttal evidence.

First, judicial authorities must actively inform suspects of their right to submit rebuttal evidence as a means of defense. Many defendants lack specialized legal knowledge and are unaware they can rebut the prosecution's claim that they "knew." This duty of notification is routinely neglected during interrogations and trials, rendering the rule ineffective. Countermeasures include ensuring full compliance through targeted awareness campaigns and strengthened internal oversight mechanisms. Second, judicial practice should clearly distinguish between the evidentiary standards for the prosecution and the defense. Considering suspects' limited capacity and resources for evidence collection, imposing the same strict burden of proof as prosecutors is unfair and unrealistic. Defendants need not meet the prosecution's "complete and conclusive evidence" standard; it suffices to present available evidence or raise reasonable doubt in the judge's mind regarding the existence of intent. Third, judicial authorities must conduct rigorous substantive reviews of all contrary evidence. The court and the procuratorate shall not reject or ostensibly reject such evidence in order to make up for the lack of investigation ability of criminal suspects. On the contrary, it is appropriate to combine the active judicial investigation of German criminal law and emphasize the characteristics of evidence to achieve inner conviction. Specifically, they must conduct in-depth verification and targeted investigations, and provide detailed reasoning about the admissibility and weight of evidence in official documents. Only this can constrain the overexpansion of the "knowledge" element and prevent unjust convictions from loose subjective determinations.

References

[1] Data sourced from "Supreme People's Procuratorate Press Conference on Enhancing Criminal Prosecution in the New Era" https: //www.spp.gov.cn/spp/xsjc/22xwfbh_sp.shtml77

[2] Data sourced from "Supreme People's Procuratorate: 64, 000 Individuals Prosecuted for Aiding and Abetting Information Network Crime in First Half of 2022" https:

DOI: 10.54254/2753-7048/2026.ZJU32770

//www.spp.gov.cn/xwfbh/wsfbt/202207/t20220722_566409.shtml#1
[3] Huang Zhongjun, Zhang Zhanying. Normative Analysis and Judicial Application of the Crime of Assisting Information Network Criminal Activities [J]. People's Procuratorate, 2021(23): 49-53.
[4] Long Zongzhi, Hu Jia. Determining "Knowledge" in the Crime of Assisting Information Network Criminal Activities [J]. Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition), 2024, 45(1): 61-72.
[5] He Jiahong. My Views on the Allocation of Burden of Proof in Criminal Procedure [J]. Politics and Law, 2002(3): 67-73. DOI: 10.15984/j.cnki.1005-9512.2002.03.012.
[6] Long Zongzhi. The Principle of Doubt in Favor of the Defendant and Its Judicial Application [J]. China Law, 2024(1): 65-84. DOI: 10.14111/j.cnki.zgfx.2024.01.004.
[7] Long Zongzhi. The Boundaries and Application of Presumptions [J]. Legal Studies, 2008(1): 106-125.
[8] Feng Mingyu. From Punishment to Governance: Goal Orientation and Normative Responses in Minor Offence Management [J]. Legal Methods, 2025, 50(1): 156-171.
[9] Liu Yanhong. Judicial Expansion Trends and Substantive Restrictions in the Crime of Assisting Information Network Criminal Activities [J]. China Legal Review, 2023(3): 58-72.
[10] Wu Hongqi. Normative Examination and Generalisation Correction of the Rules for Determining Knowledge in the Crime of Assisting Information Network Crime Activities [J]. Forum of Jurisprudence, 2025, 40(2): 17-27.
[11] Li Yongchao, Wang Li. Determining Subjective Knowledge and Serious Circumstances in the Crime of Assisting Information Network Criminal Activities [J]. People's Judiciary, 2021(35): 24-26. DOI: 10.19684/j.cnki.1002-4603.2021.35.027.
[12] Jiang Luoyi. Judicial Determination of "Knowledge" in the Crime of Assisting Information Network Criminal Activities from a "Dual Nature" Perspective: A Study Based on 1, 082 Relevant Judgments [J].Journal of Jurisprudence, 2025, 46(5): 73-93. DOI: 10.16092/j.cnki.1001-618x.2025.05.001.