

On the Generalization of the Determination of "Knowing" in Crimes of Concealment and Its Rectification in the Internet Era

Rongna Ma *

Law School, Hebei University of Economics and Business, Shijiazhuang, China

* Corresponding Author Email: mrn131814@outlook.com

Abstract. With the in-depth development of information network technology, criminal activities have undergone a transformation towards networking, and the application of the crime of concealing and covering up has expanded sharply in the internet era. However, in judicial practice, the determination of the core element "knowing" of this offense has shifted from "comprehensive assessment" to a trend of "simple presumption," leading to widespread controversy among both theoretical and practical circles. This paper, against the backdrop of the judicial application of money laundering crimes in the internet era, systematically examines the specific manifestations, underlying causes, and corrective measures of the generalized interpretation of "knowing." It proposes the construction of a systematic "concept-rules-institution" framework: Shift towards conservative and restrained judicial stance, strictly implement the principle of doubt favoring the defendant. Clarify the difference between the crime of concealment and the crime of aiding and abetting in the recognition rules, strictly establish the threshold and comprehensive review procedures. Through measures such as refining judicial interpretations, issuing guidance cases, and strengthening training for judicial personnel, people ensure the standardization and uniformity of the identification process in terms of institutional safeguards. Research suggests that only by adhering to the principle of unity of subjectivity and objectivity, and achieving refined and hierarchical identification, can people achieve a legal balance between effectively combating cybercrime and safeguarding citizens' rights.

Keywords: Crime of concealment; Knowing; recognition of generalization; comprehensive recognition; cybercrime.

1. Introduction

With the deep embedding and rapid iteration of information network technology, human society is undergoing an unprecedented digital transformation. The iteration of digital technology and the expansion of cyberspace have not only reshaped the forms of social interaction and economic activities but also spurred the networked transformation of criminal behavior. Among them, the crime of concealing, concealing criminal proceeds, and profits from criminal proceeds (hereinafter referred to as "concealment crime"), as an important channel for downstream crimes to "sell stolen goods", has shown a rapid expansion trend in its application in the Internet age and plays an increasingly important role in combating downstream crimes [1]. In 2023, the national procuratorial organs prosecuted a total of 137386 people for the crime of concealing "two cards", a year-on-year increase of 66.2%, making it the second largest telecommunications network fraud related crime after the crime of aiding and abetting. In judicial practice, the determination of the core constituent element of the crime of "knowing" has shown a tendency to shift from "comprehensive determination" to "simple presumption", which has sparked widespread controversy in both academia and practice. In relevant documents, it is mentioned that in practice, there is a tendency to lower the standard of proof, mechanically apply presumption rules, confuse minor and serious crimes, invert the burden of proof, and expand the generalization and abuse of abnormal interpretation situations in the determination of the crime of concealment [2]. Scholars point out that the phenomenon of generalization deviates from the principles of responsibility and legality in criminal law, which may lead to "objective attribution" and violate the legitimacy of punishment. The causes of generalization are complex and diverse, which is not only a utilitarian choice to address the problem of proving cybercrime, but also a continuation of the traditional thinking of "heavy crackdown, light protection" in judicial practice. Scholars believe that the causes of generalization are multifaceted.

Firstly, the path dependence of judicial practice. When facing massive cases of cybercrime, judicial practice sometimes relies on "presumed knowledge" in pursuit of efficiency, forming a "one size fits all" approach to convenient criminalization [3]. Secondly, there are technological challenges in cybercrime, such as the anonymity and cross regional nature of the internet, as well as the detailed division of labor in the black industry chain, which make it extremely difficult to obtain direct evidence of the subjective intent of the perpetrator. The explanatory power of traditional accomplice theory is insufficient in this context, proving that "knowing" is very difficult. Furthermore, due to the confusion of the requirements for the connotation of "knowing" between serious and minor offenses, the standard of proof for the crime of concealment has been lowered. Finally, in practice, there is often a phenomenon where judges use "common sense" to apply fallback clauses, leading to subjective and arbitrary criteria for determination.

Therefore, how to maintain a high-pressure situation against cybercrime while adhering to the spirit of criminal law modesty and the principle of criminal responsibility and effectively rectify the generalization of the recognition of "knowing" has become a major issue that urgently needs to be responded to by the theoretical and practical circles. This article systematically sorts out the evolution of the recognition of "knowing", clearly defines its generalization performance, and explores reasonable correction paths. It not only has significant theoretical value but also has urgent practical significance for unifying judicial standards and safeguarding citizens' rights.

2. The Current Situation and Alienation Cause of the Generalization of the Recognition of "Knowing" in the Crime of Concealment in the Internet Age

2.1. The Current Judicial Situation of the Generalization of the Recognition of "Knowing"

The expression 'knowing' is hollow in content and has too broad an extension. The general theory of criminal law holds that "knowing" in the crime of concealment includes "knowing" and "ought to know", usually interpreted as explicit knowledge and highly probable knowledge [4]. In criminal law practice, the 'knowing' of the crime of concealment includes explicit knowledge and presumed knowledge (often expressed as 'ought to know' in judicial practice). 'ought to know' is the intention inferred through objective evidence, rather than the 'ought to foresee' in negligence. However, in the judicial practice of handling cases related to the crime of concealment, the concept of "should have known" is often confused with the concept of "should have foreseen" in negligent crimes, resulting in an excessive extension of the recognition of "knowing" in the crime of concealment and blurring the boundary between intention and negligence [5]. In judicial practice, the mechanical application of the presumption rule of "knowing" leads to the unlimited expansion of general knowledge. Grassroots judicial organs, under the pressure of having too many cases and too few people, often equate abnormal situations such as "charging significantly higher fees than the market" listed in judicial interpretations with subjective knowledge, ignoring the possibility of the perpetrator's defense and counter evidence, violating the requirement of judicial interpretations to combine cognitive ability, past experience, and other comprehensive judgment of the entire case evidence, and turning presumption into a tool for conviction, resulting in factual misidentification. At the same time, knowing that there is a risk of reversal of the burden of proof. The presumption rules set by relevant documents have been alienated in practice as a sufficient condition for knowledge based on a single abnormal situation. Despite the limitation of "excluding those with evidence proving ignorance", the burden of proving innocence is essentially transferred to the defendant. The defense put forward by the defendant, such as "thinking it was a legitimate part-time job," is often not accepted due to the difficulty in providing conclusive evidence, which undermines their right to provide counter evidence and violates the basic principle of the prosecution bearing the burden of proof.

2.2. The Alienation Causes of the Generalized Phenomenon of "Knowing Well" Recognition

The causes of the generalization of "knowing" in the internet age are multi-level and systematic. On a theoretical level, the traditional theory of accomplice focuses on a clear intention connection, which makes it difficult to explain the atypical collaborative mode of fine division of labor and loose cooperation in online black industries. When a subjective connection is difficult to prove, it relies on the broad recognition of "knowing" to achieve accountability [6]. On an objective level, the use of technologies such as encrypted communication and virtual assets has made behavior increasingly "de-subjective" and "technology-neutral", obscuring internal criminal intent, and hindering the traditional path of proof that relies on oral testimony and direct behavioral representation [7,8]. At the level of judicial practice, the massive number of online black industry cases involving multiple stakeholders brings efficiency pressure, and judicial authorities tend to adopt standardized presumption models to improve efficiency, forming a path dependence on simplified processing [9]. At the level of institutional incentives, the heavy punishment orientation under the competition of charges has a distorted effect, and there is a significant difference in the statutory punishment between the crime of aiding and abetting and the crime of concealing. Some cases have experienced the alienation of "sentencing to counter conviction"[10]. Liu Yanhong pointed out that in practice, there are situations where non-core payment settlement behaviors are identified as payment settlements by analogy, expanding the scope of assistance behaviors [11].

3. Legal Criticism and Risk Estimation of the Generalization of the Recognition of "Knowing"

Firstly, knowing expanding the scope of criminal punishment due to improper generalization undermines the principle of modesty in criminal law. When "should know" and "may know" are simply equated with "knowing", the boundary between crime and non-crime is blurred, and some cases of negligence, carelessness, negligence, and only vague vigilance towards the nature of the behavior are included in the scope of intentional crime crackdown. Relevant experts point out that it is necessary to understand "knowing or should have known" from the perspective of criminal integration, which belongs to intentional cognitive factors. If mistakenly classified as "should have foreseen" in negligent crimes, it will confuse the boundary between intention and negligence and trigger the risk of "objective attribution"-As long as assistance is objectively provided for the upstream crime and there are abnormal manifestations, subjective intent is presumed, which not only lowers the threshold for conviction, but also loosely grasps quantitative elements such as "serious circumstances", making the criminal law network tighten both qualitatively and in terms of the degree of harm.

Secondly, vague and broad standards of knowledge inhibit technological innovation and the development of normal market formats. Third party payment, cloud server leasing and other network technology services themselves have neutrality and legitimacy, but judicial practice often infers knowledge from external characteristics such as "abnormal transactions", which expose a large number of normal service providers to unforeseeable criminal risks. Operators may excessively review users, refuse high-risk legal innovative businesses, or exit the market to avoid risks, which will constrain the development of the digital economy and hinder the exploration of technology driven emerging business models [12].

Finally, knowing that simplification and weak reasoning erode judicial legitimacy and credibility. Criminal conviction needs to be based on solid evidence and rigorous logic, but under the trend of generalization, some judicial documents simplify and template the reasoning of knowing and identifying, without considering the comprehensive evaluation of the perpetrator's cognitive ability, professional background, etc., and directly apply judicial interpretations [13]. This not only deprives the defendant of their right to effective defense but also makes the judgment difficult to convince the public and violates the criminal procedure principle that the prosecution bears the burden of proof. The source of judicial credibility lies in procedural fairness and substantive justice. Although hasty

determination may have short-term effects, it will damage the fundamental trust of the public in respecting the law and protecting human rights in the long run. Its rectification is related to the foundation of judicial authority and the belief in the rule of law.

4. Systematic Legal Correction Measures for the Generalization of the Recognition of "Knowing"

In response to the problems caused by the generalization of the recognition of "knowing" in the context of the Internet, this requires the coordination of judicial stance, recognition rules, and supporting systems to achieve a fundamental transformation from pursuing efficiency in cracking down unilaterally to adhering to the precision and fairness of criminal law.

4.1. The Transformation of Judicial Stance from "Active Expansion" to "Conservative Restraint"

People must promote a profound transformation of the judicial stance from "active expansion" to "conservative restraint". The core of this transformation is that in the application of the presumption of "knowing", the basic principle of criminal procedure of "favoring the defendant in case of doubt" must be strictly implemented. This means that when inferring subjective "knowing" based on objective abnormal behavior, if there is a reasonable doubt about the conclusion drawn, a favorable determination should be made for the defendant, and the standard of proof should not be lowered in pursuit of conviction. People must be vigilant against the phenomenon of "only focusing on the abnormal performance of a certain objective behavior and ignoring the principle of comprehensive determination" in practice, as well as the resulting "one size fits all" thinking inertia of convenient conviction. At the same time, the principle of modesty in criminal law should be fully introduced and practiced. For the auxiliary behaviors of online gray and black products that are subjectively ambiguous and have social harm on the edge of crime or non crime, priority should be given to handling them through non criminal means such as civil compensation and administrative penalties. This is in line with the current judicial concept of "equal emphasis on crime and governance", aiming to avoid negative effects such as "labeling" caused by the "uniform sentencing" of minor crimes through restraint and tolerance in the judicial process. To this end, people should actively explore the connection of execution, that is, for behaviors that do not constitute a criminal offense but violate administrative law, transfer them to administrative organs for administrative penalties, achieve hierarchical investigation of legal responsibility, establish a case guidance library for "knowing" identification, and make quantitative provisions for the specific circumstances of "abnormal transactions" in the crime of online concealment (such as the deviation range of transaction prices and the speed of fund circulation), to avoid subjective speculation by judicial personnel.

4.2. Establishing Clear Rules for Determining and Inferring Knowledge

Clarify the difference in the standard of 'knowing' between the crime of concealment and the crime of aiding and abetting - the crime of concealment requires 'clear knowledge that the funds are proceeds of crime', while the crime of aiding and abetting only requires 'general knowledge that they may be used for cybercrime', and the differentiation of criminal boundaries is used to curb the alienation tendency of 'elevated recognition'. Efforts should be made to build a clear and strictly limited system of rules for determining and inferring knowledge. Firstly, a high threshold must be set for "presumed knowing" and sufficient rights to counter evidence must be guaranteed. People must firmly eliminate the tendency of purely objective attribution and prohibit using single circumstances such as "inter provincial transactions," "rapid transfers," and "abnormal transaction prices" as sufficient conditions for determining "knowing". Secondly, it is necessary to standardize the operational process of judicial recognition and establish a recognition model of "comprehensive review + elimination of doubts". Judicial personnel should comprehensively examine multidimensional factors such as the perpetrator's cognitive ability, past experiences, professional

background, specific context of behavior, relationship with upstream criminals, and the reasonableness of their explanation of abnormal situations, to ensure that the final conclusion can exclude reasonable suspicion. Thirdly, it is necessary to clarify and coordinate the boundary between administrative violations and criminal offenses, and be wary of the phenomenon of "execution hanging". In terms of program design, before proposing the prosecutorial opinion on transferring administrative penalties, the procuratorial organs should carefully review the qualitative and quantitative punishment circumstances and the necessity of punishment of illegal behavior, to ensure that the punishment is not excessive.

4.3. Improving Supported Institutional Safeguards

It is necessary to improve relevant supporting systems to ensure the effective implementation of rectification measures. Firstly, the highest judicial authority should issue more detailed judicial interpretations or authoritative guidance cases for the controversial charges of "knowing" such as aiding and abetting, concealing, etc., clarifying the core elements, proof standards, and typical situations that do not constitute "knowing", in order to unify the judgment standards nationwide. The Supreme People's Procuratorate has played a demonstrative role in correcting errors in the application of the law and unifying the standards for evidence review and judgment by issuing typical cases of criminal prosecution. This practice should be continued and strengthened. Secondly, strengthening the training of judicial personnel, correct misunderstandings of "knowing" and "should know", and enhance their comprehensive review and judgment abilities. Establish a mechanism for evaluating the quality of cases, including the reasonableness of the determination of "knowing" in the scope of evaluation, and forcing judicial personnel to standardize the application of rules. In summary, the correction of the generalization of the recognition of "knowing" is a systematic project that concerns the basic principles of criminal law, confidence in judicial fairness, and the vitality of the digital economy. Only by returning to humility and prudence in judicial concepts, adhering to comprehensive recognition and strict proof in rule design, and strengthening guidance and supervision in institutional safeguards, can a solid legal balance be established between effectively combating cybercrime and resolutely safeguarding citizens' rights.

5. Conclusion

In summary, this article systematically analyzes the manifestation and causes of the generalization of the judicial determination of the core element "knowing" in the context of the application of the crime of concealment in the Internet age. This generalization phenomenon blurs the boundary between intention and negligence, improperly expands the scope of criminal punishment, inhibits the development of technology neutral industries, and deeply erodes judicial rigor and credibility. To rectify this phenomenon, people should abandon scattered repairs and construct a three in one systematic plan of "concept rule system": shift towards a conservative and restrained stance of adhering to modesty in terms of ideology. Establishing clear identification criteria in terms of rules and strictly establish thresholds for inference. Systematically, people ensure the implementation of judicial interpretations and strengthen training. In the era of the internet, criminal justice needs to balance the efficiency of prosecution and the protection of rights, and the determination of "knowing" is a key field. Only by adhering to the unity of subjectivity and objectivity, precise and refined identification, can people avoid objective attribution, ensure the legitimacy and necessity of punishment, and serve the dual goals of network security and digital economy development.

References

- [1] Financial Action Task Force on Money Laundering. FATF Recommendations. 2021.
- [2] The fourth court of criminal trial in the Supreme People's Court. Understanding and application of Interpretation on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Concealing, Concealing and Gaining from Crime. 2025.
- [3] Zhou Yuanyuan, Zhang Lei, Yao Senbo. Practical Dilemma and Judicial Response of "Two Cards" Crime. *Journal of Beijing University of Science*, 2025, 41(6): 81-90.
- [4] Liu Xianquan, Fang Huiying. Difficult to identify the crime of helping information network criminal activities. *People's Procuratorate*, 2017, (19): 9-12.
- [5] Ma Jinghua, Yuan Jiaqian. On the presumption of subjective knowledge and its standardization path to identify the subjective knowledge of the judicial interpretation of the bottom clause as the starting point. *Journal of Guizhou Minzu University (Philosophy and Social Sciences Edition)*, 2024, (4): 132-148.
- [6] Manning M, Akartuna E A, Johnson S D. Opportunities to future crime: Scoping the future of money laundering and terrorist financing through cryptoassets. *Technological Forecasting and Social Change*, 2025.
- [7] Robin Booth, Simon Farrell, Nicolas de Boynes, et al. *Money Laundering Law and Regulation: A Practical Guide*. Oxford University Press. 2021.
- [8] Skinner C P. Coins, cross-border payments, and anti-money laundering law. *Harvard Journal on Legislation*, 2023.
- [9] Wang Shenghua, Jiang Chenyan. The academic division of criminal law doctrine of "helping the letter" and "concealing the truth". *Journal of Hefei University*, 2025, 42(1).
- [10] Liu Yanhong. The trend of judicial expansion and substantial limitation of the crime of helping information network criminal activities. *China Law Review*, 2023, (3).
- [11] Wu Hongqi. Rule review and generalization correction of the crime of aiding faith. *Law Forum*, 2025, 40(2): 17-27.
- [12] Akartuna E A, Johnson S D, Thornton A. A holistic network analysis of the money laundering threat landscape: Assessing criminal typologies, resilience and implications for disruption. 2025.
- [13] Wang Xing. Continuation of the Criminal Procedure Law of Knowing Presumption Proof. *Contemporary Law*, 2025, (4).