The Narrowing of the Definition of the Crime of Helping Information Network Criminal Activities

Zheng Wang *

School of Law, East China University of Science and Technology, Shanghai, China

* Corresponding Author Email: wzzz63455@gmail.com

Abstract. Since the crime of helping information networks was established in 2015, criminal activities have played a significant role in combating the cybercrime chain. With the increased crackdown on cybercrime in recent years, the number of prosecutions for this crime has surged, exhibiting a serious trend of "pocketization" expansion. The core reasons for this lie in the dual generalization of the subjective and objective elements of the crime, the mechanical determination of serious circumstances, and the improper handling of concurrence elements. Drawing on the international experience of the US's "willful blindness" and "Hierarchical Voluntary Sentencing Guidelines" , and the UK's "culpability and harm matrix" and "authorized disclosure" exemption, this article argues for the need to reconstruct the determination of the elements of the crime of helping information network criminal activities .Regarding the subjective elements, it is necessary to narrow down "knowing" to explicit knowing and presumed knowing, and to raise the standard of proof for presumed knowing based on the "willful blindness" standard, and to construct a clear path to acquittal by referring to "authorized disclosure"; for the circumstances of the crime, adhere to the dual sentencing review, and replace the sole criterion of amount with a comprehensive evaluation; and clarify the boundaries of concurrence based on subjective standards.

Keywords: Cybercrime; the crime of helping information network criminal activities; appropriation of specific categories; narrowing of pathways.

1. Introduction

The rapid development of information network technology has reshaped social ecology, but it has also provided a new field for crime, and traditional legislation is gradually becoming ineffective in combating the surge in cybercrime. In 2015, China added Article 287-2 to the Ninth Amendment to the Criminal Law, establishing the crime of helping information network criminal activities to regulate acts of knowingly providing payment settlement, internet access, or other assistance to others who use information networks to commit crimes, where the circumstances are serious.'

In the cybercrime chain, technology supporters and upstream criminals often lack clear "collusion" or criminal intent, making it difficult to prosecute them as joint criminals. Therefore, the purpose of establishing this crime is to formalize cybercrime aiding and abetting based on knowing of unspecified criminal acts, and to fill the gaps in the protection of legal interests that the existing theory of complicity cannot cover [1].

However, this crime has been over-applied in judicial practice. In recent years, with the advancement of the "Card Breaking" campaign to combat crimes involving "two cards" (illegally renting, selling, and purchasing phone cards, bank cards, and related illegal and criminal activities), the number of cases involving aiding and abetting crimes has surged, becoming one of the top five crimes nationwide and gradually becoming a "pocketization" crime in the governance of cybercrime. This trend of "pocketing" has seriously impacted on the principles of restraint in criminal law and the legality of punishment, posing a challenge to the protection of human rights in the judiciary.

Currently, the main theories in academia regarding the crime of helping information network criminal activities are as follows. The neutral aiding and abetting theory hold that the crime is a criminal offense punishable by law for providing assistance in network services; the sentencing rule theory holds that the crime is a sentencing rule for helping in network crimes, rather than an independent principal offense; and the accomplice principal offense theory holds that the crime is to

evaluate the original accomplice behavior in network crimes as an independent principal offense [2-4].

However, this article tends to believe that the crime of helping information network criminal activities does not rely on the traditional theory of complicity but is based on the criminalization of online helping behavior with unspecified criminal knowing. Specifically, the underlying reason for the expansion of the crime of helping information network criminal activities lies in the structural imbalance in its application to criminal law. Based on this, this article analyzes the reasons for the expanded application of the crime of helping information network criminal activities money laundering from the perspective of the elements of the crime and the handling of the competitive relationship. It also provides extraterritorial experience for the narrowing of the crime of helping information network criminal activities money laundering by combining the regulatory experience of the United Kingdom and the United States on money laundering.

2. Causal Analysis: Structural Imbalance in the Expansion of Application

The open-ended nature of the elements constituting the crime of helping information network criminal activities provides room for judicial expansion, leading to a loss of control over both subjective and objective aspects.

2.1. Generalization and Expansion of Constituent Elements

The "dilution" of the subjective element crosses the line of "knowing" Criminal law requires "knowing" that another person is using information networks to commit a crime. "Knowing" refers to the actor having a clear understanding or being presumed to know by the court. It does not require the actor to know the specific type of upstream crime, nor does it require the actor to have a common criminal intent with the upstream criminal. Rather, it means that the actor generally knows that his or her actions may help cybercrime. The judicial interpretation provides clear provisions regarding presumed knowing, such as when the transaction price or method is obviously abnormal, or when assistance is provided after being notified by the regulatory authorities. In practice, in order to reduce the burden of proof, the "knowing" standard has been seriously diluted. The law enforcement agencies often improperly equate "knowing" with "should have known" or "may have known" and rely excessively on phenomena such as abnormal transactions and high returns to make presumptions and lack sufficient counter-evidence mechanisms. This practice makes it easy for negligent or even neutral behavior to be included in the category of intentional crime, breaking through the legal boundaries of intent [5].

The "generalization" of objective behavior and the abuse of pocketization clauses. Regarding the circumstances of assistance stipulated in the crime of helping information network criminal activities, the Criminal Law only generally stipulates "technical support such as Internet access, server hosting, network storage, and communication transmission, or providing advertising promotion, payment settlement, etc.", without specifying the specific manifestations of these behaviors, which constitutes an open-ended element of the crime. Meanwhile, regarding the most common payment and settlement behavior in the crime of helping information network criminal activities fraud, the judicial interpretation only provides a reverse list, pointing out that if the perpetrator "only rents or sells credit cards" to receive fraudulent funds, without carrying out transfers, cash withdrawals, or providing verification services such as facial recognition, it is not appropriate to identify it as aiding and abetting payment and settlement. However, this has not helped to narrow down the objective elements of the crime of helping information network criminal activities. In practice, law enforcement agencies tend to interpret this broadly, and providing WeChat/Alipay QR codes, providing WeChat accounts, helping to unblock WeChat accounts, or even providing labor services will all be classified as the crime of assisting in the crime of fraud. In addition, for indirect assistance, such as when a person helps another person find someone willing to provide a bank card for settlement, if the latter

constitutes the crime of assisting in the crime of fraud, the former will also be considered an accomplice to it [6].

2.2. Mechanized Identification of Serious Circumstances

The crime of aiding and abetting fraud uses "serious circumstances" as the threshold for conviction, but judicial determination of this lacks substantive judgment. Judicial authorities rely solely on mechanical standards such as "three or more parties" and "payment settlement amount exceeding 200,000 yuan" as the basis for conviction, and meeting even one of these standards is sufficient for conviction, making the threshold extremely low. This method of determination ignores substantive factors such as the degree of harm to legal interests caused by the act and the subjective malice of the actor. Furthermore, the crime of helping information network criminal activities takes the form of "accumulated amount to constitute crime", but the act of helping is a collection of multiple people and multiple stages, not a continuous act of the individual actor. The settlement amount is often not under the control of the actor, which can easily lead to objective criminalization [7].

2.3. Mishandling of Competitive and Cooperative Relationships Leading to Abuse of the Safety Net

The improper handling of the overlapping relationship between the crime of helping information network criminal activities crimes and the crimes of complicity in upstream crimes and concealment of crimes is a systemic flaw in its "catch-all" approach.

Concurrent involvement with upstream crimes. When dealing with the relationship with upstream crimes such as fraud, due to the lack of clear evidence of "collusion of criminal intent," judicial authorities tend to simply deny the accomplice relationship and directly apply the charge of helping. This has led to many cases that should have been prosecuted as accomplices in fraud with higher statutory penalties being ultimately settled as the crime of helping information network criminal activities with lower statutory penalties, resulting in a phenomenon of "serious crimes being punished lightly"[8].

It overlaps with the crime of concealing. The “payment and settlement” in the crime of helping information network criminal activities and the “transfer of funds” in the crime of concealing and disguising are highly overlapping in meaning. In practice, courts often adopt the simple approach of "simultaneous offenses, i.e., lighter punishment" and directly apply the crime of helping information network criminal activities, which has a lower statutory penalty. This has resulted in a large number of facts that meet the elements of the crime of concealment being "leaked" into the pocket of the crime of helping information network criminal activities, leading to confusion in the criminal system and an imbalance in the gradient of punishment.

3. Learning from Experiences Abroad

The experience gained by other countries in regulating aiding and abetting online money laundering and other related activities provides a reference for narrowing the definition of aiding and abetting crimes.

3.1. Lessons Learned from Subjective Determination and Exoneration Mechanisms

The United States has introduced the principle of "willful blindness" as a presumed evidence strategy for money laundering. The theoretical basis of this mechanism is that “willful blindness” can be a permissible substitute for “actual knowing”, which helps to deal with the strategy of criminal groups using “blind spots” to evade responsibility [9]. In the context of money laundering, this strategy emphasizes that the defendant’s intentional avoidance must exceed reasonable doubt and is similar to indirect intent, effectively preventing professional criminals from profiting by intentionally maintaining ignorance [10]. In practice, the prosecution needs to prove that the suspect had the intention to deliberately evade the facts of the crime, rather than simply being negligent or careless.

This presumption is not absolute. The system provides the defendant with sufficient rebuttal mechanisms, allowing them to overturn the prosecution's charges by proving that due diligence has been carried out (such as background checks on clients or reporting suspicious activities), thereby upholding due process and the rights of the defendant and avoiding excessive punishment.

In United States vs. Gyanendra Asre (2024), the defendant Asre, as the anti-money laundering compliance officer and expert of the credit union, deliberately ignored red lines for international transactions (such as bulk cash deposits of more than $100 million from high-risk jurisdictions such as Mexican banks and serial checks) and failed to implement AML procedures or file SAR/CTR reports. The court found him guilty of "willful blindness" because, as an expert, his deliberate avoidance of his duties demonstrated a subjective intent to evade the facts of the crime, rather than mere negligence. This ruling upholds the positive role of "willful blindness": it ensures that compliance experts cannot use "ignorance" as an excuse to evade responsibility.

The UK employs an "Authorised Disclosure" exemption mechanism. To prevent internet service providers from being implicated in money laundering through "passive assistance," UK law has created an "authorized disclosure" exemption: criminal liability can be blocked as long as the perpetrator submits a Suspicious Activity Report (SAR) to the National Crime Agency (NCA) and obtains consent before the transaction is completed, providing a clear path to acquittal for payment platforms, escrow service providers, crypto mixers, and others.

3.2. Reference to Sentencing Standards

The U.S. Federal Sentencing Guidelines employ a "hierarchical" approach to aiding and abetting money laundering, requiring that the basic crime level be determined based on the value of the funds involved. The larger the amount of money, the higher the sentencing level. The guidelines also adjust the level of punishment based on factors such as whether the perpetrator is involved in "professional money laundering," whether "complex money laundering" is involved, and whether the perpetrator was aware that the funds originated from specific serious crimes (such as drugs or violent crimes).This directly corresponds to the definition of "serious circumstances" in China's "crime of aiding and abetting",transforming it from a mechanical number of cases or amount of money into quantifiable harmful consequences. The guidelines mandate the application of "role adjustment" during the sentencing phase. For "minimum participants" like the student who sold the cards, the guidelines explicitly allow for significant reductions in sentencing (-4 levels) to ensure that the punishment matches the defendant's actual responsibility and subjective culpability in the crime.

The UK uses a "culpability and harm matrix". The UK has achieved proportional sentencing for low-level money mules through the Sentencing Commission guidelines, thus avoiding an imbalance in punishment. In sentencing, judges must follow the "culpability and harm matrix." In terms of culpability, the focus is on the defendant's role, intent, and subjective malice.Money mules are usually classified as having "lower culpability". The main considerations for determining the harm are the amount of money involved, the duration of the crime, and other criminal consequences. In the 2024 money mule money laundering case heard in Swindon Crown Court, six defendants (including Serena Hodge, Patrick Egan, etc.) were convicted of acting as money mules to help defraud the elderly and launder approximately £250,000.They were identified as low-culpability participants, and the court sentenced them to lower sentences based on a culpability and harm matrix: Hodge received 18 months' imprisonment, two years' probation, and 150 hours of unpaid work; Egan received two years' imprisonment; and the others received community orders, and unpaid work. Therefore, even if the amount of money involved is huge, once the crime is deemed minor, the starting point for sentencing will fall in the lowest range of the matrix, usually resulting in a suspended sentence or a very short period of imprisonment, reflecting a balance between punishment and individual case justice.

4. The Restricted Path of "Pocketing" the Crime of Helping Information Network Criminal Activities

Based on the above analysis and overseas experience, this paper proposes the following three paths to limit the crime of helping information network criminal activities.

4.1. Reconstructing Subjective Knowing and Constructing a Pathway to Acquittal

Strictly define the presumption standard for "knowing". Drawing on the American theory of "intentional ignorance", "knowing" can be identified as "explicit knowing" and "presumed knowing", but "presumed knowing" is by no means equivalent to "should have known", "may have known", or even negligence. It is a procedural proof strategy and must be based on reasonable judgment of evidence and facts. Therefore, China needs to clarify the standard of proof for presumed knowing: requiring the prosecution to prove that the actor "intentionally avoided knowing" rather than simply "negligence", and providing the parties with a "rebuttal mechanism" to fully prove that they were indeed unaware [11, 12].

Establish a localized "authorized disclosure" mechanism for acquittal. The newly released judicial interpretation on the crime of helping information network criminal activities in 2025 establishes a "linkage between administrative and criminal law enforcement and non-prosecution" approach to acquittal, but does not provide a clear channel for this approach. China could learn from the authorized disclosure mechanism of POCA 2002 s.338 in the UK, opening relevant online disclosure channels, defining the disclosing entities as network service providers and those who conduct the transfers, the receiving agency as the cybersecurity department of the public security organ, and the disclosure deadline as within 24 hours. Once the receiving agency confirms the facts, it can issue a receipt to the discloser that has the effect of preventing criminal liability.This measure not only allows individuals to avoid concealing their crimes or being forced to continue committing them due to the lack of a clear path to innocence when they realize their actions may aid in the crime, but it also allows public security organs to obtain case leads as soon as possible, thereby improving the efficiency of case handling.

4.2. Replacing Sole Reliance on Monetary Value with Comprehensive Review of the Circumstances

The principle of "dual sentencing" needs to be established. The culpability is divided into the sentencing of the predicate offense and the sentencing of the aiding and abetting act. The predicate offense must meet the sentencing requirement of "being investigated and prosecuted" or "being verified as true". The amount of the aiding and abetting act should be reduced by the amount of legitimate funds and duplicate transfers. Currently, there are two major misconceptions in the practice regarding the determination of serious circumstances.Firstly, the "principal crime" is rendered meaningless; second, the "assistance crime" is overgeneralized. In response, a "double-crime" review should be adhered to: first, the principal offender's conduct needs to be reviewed for the degree of guilt; the establishment of the crime of helping information network criminal activities requires that the principal offender's conduct constitute a crime, unless the act of aiding and abetting involves multiple upstream offenders, in which case an exception can be presumed. Secondly, the severity of the crime of helping information network criminal activities must be examined. The amount of the crime for aiding and abetting must be directly linked to the funds involved in the crime. It is prohibited to directly include simple transaction records or repeated transfers, and to replace mechanical standards with illegal connections.

Furthermore, the determination of "serious circumstances" should be broken down into two stages: "qualitative" and "quantitative." First, independently determine whether the act of aiding and abetting creates an abstract danger worthy of criminal punishment (substantive preparatory offense), and then determine whether it reaches the threshold of the amount or number of persons for the crime stipulated

in the article; only after completing the qualitative filtering can the crime be calculated, to prevent direct criminalization based solely on the amount.

Introducing a "Hierarchical Sentencing System". Drawing on US experience, construct a tiered benchmark sentencing for aiding and abetting crimes. Sentencing should be adjusted comprehensively based on multiple factors, including the amount of crime, the number of victims, the nature of the predicate offense, and whether the perpetrator possesses professional expertise. Replace the single standard of the amount of crime with an assessment of substantial harm, achieving proportionality between crime and punishment.

4.3. Clarifying Concurrence of Criminal Charges and Standardizing Judgment Procedures

The degree of "knowing" is used to clarify the boundaries of accomplices. Knowing is divided into knowing of the nature of the predicate crime and complete knowing of both the nature and methods of the predicate crime. As long as the behavior is recognized as "information network crime", the crime of helping information network criminal activities can be satisfied. However, if the specific methods and procedures of the crime are known, the evaluation of accomplices should be returned. Thus, "vague cognition" (knowing that the behavior may help network crime, but not knowing the specific type or method of the crime) is left in the pocket of aiding and abetting, while "precise cognition" (knowing the specific type (such as fraud), method or procedure) of the upstream crime is returned to the upstream crime [13].

The distinction between concealment and cover-up is clarified by the concept of "collusion." For the crime of concealment, "prior collusion" serves as the dividing line: if there is only an agreement to transfer embezzled funds beforehand without collusion, it should be consideredthe crime of helping information network criminal activities; if a stable cooperative relationship has been formed, it should be evaluated as the crime of concealment [14].

5. Conclusion

This paper uses a combination of normative analysis and empirical research to analyze the causes of the judicial expansion of the crime of helping information network criminal activities cybercrime. It concludes that its "pocketization" nature stems from the generalization of the elements of the crime, the mechanical determination of serious circumstances, and the improper handling of Concurrence. Furthermore, it elaborates on the impact of this expansion trend on the principles of restraint in criminal law and the principle of legality in criminal law. To address this issue, this paper analyzes the handling of money laundering, aiding and abetting in common law countries, delving into the methods of subjective identification, pathways to acquittal, and sentencing regulations. Based on this, three restrictive pathways are proposed. First, it references the US standard of "intentional ignorance" to clearly presume knowing and construct related pathways to acquit crimes. Second, it optimizesconstruct the determination of circumstances, adheres to dual sentencing review, substitutes substantial harm for monetary value, and constructs a tiered, floating sentencing system. Third, it distinguishes the Concurrence between aiding and abetting crimes and other crimes through the "degree of knowing." The combination of these three methods constitutes a three-pronged governance framework of "subjective-objective-procedural." This framework enables a precise narrowing of the crime of helping information network criminal activities, restoring it to its auxiliary and supplementary legislative role. This approach effectively combats cybercrime while genuinely protecting human rights and upholding the fairness and harmony of the criminal law system.

References

[1] Lu J, Yan E P. The legislative positioning and identification of the crime of helping information network criminal activities: Empirical evidence, theory, and rules—Based on 26 criminal second-instance corrective judgments. Criminal Law Review, 2023, 75(3): 1-26.

[2] Li C B. A new discussion on the boundary of criminal punishment for neutral network helping behaviors—From the perspective of the crime of helping information network criminal activities. Legal Science Magazine, 2020, 41(4): 79-89.

[3] Zhang M K. On the crime of helping information network criminal activities. Politics and Law, 2016, (2): 2-16.

[4] Chen X L. The principalization of accomplice behavior: From the perspective of the crime of helping information network criminal activities. Journal of Comparative Law, 2022, (2): 44-58.

[5] Liu Y H. The judicial expansion trend and substantive restriction of the crime of helping information network criminal activities. China Law Review, 2023, (3): 58-72.

[6] Mo H X, Lü X. On the judicial expansion and normative application of the crime of helping information network criminal activities. Journal of Guizhou Normal University (Social Sciences Edition), 2023, (1): 123-138.

[7] Jing L J. The application of the "circumstances are serious" clause of the crime of helping information network criminal activities from the perspective of two-stage illegality judgment. China Applied Jurisprudence, 2025, (4): 83-96.

[8] Wang Y Q. Research on the concurrence issues related to the crime of helping information network criminal activities. Legal Forum, 2025, 40(2): 28-41.

[9] Von Kaenel F J. Willful blindness: A permissible substitute for actual knowledge under the Money Laundering Control Act. Washington University Law Quarterly, 1993, 71: 1189.

[10] Guzman S, Pucheta S D. Money laundering and willful blindness. Revista Jurídica Austral, 2024, 5: 505.

[11] Wang Z Y. The normative purpose and judicial application of the crime of helping information network criminal activities. China Applied Jurisprudence, 2025, (4): 70-82.

[12] Wang H W. The judicial misunderstandings and theoretical corrections of the crime of helping information network criminal activities. Journal of Finance and Law, 2024, (5): 179-192.

[13] Jiang L Y. The judicial identification of "knowledge" in the crime of helping information network criminal activities from the perspective of "duality"—Based on 1,082 relevant judgments. Legal Science Magazine, 2025, 46(5): 73-93.

[14] Yan E P. The legislative interpretation and judicial correction of the crime of helping information network criminal activities. Science of Law (Journal of Northwest University of Political Science and Law), 2024, 42(5): 117-128.