Proceedings of the 2nd International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2024.20818

A Brief Analysis of the Application of the Restrictive Position in the Offense of Aiding Information Network Criminal Activities

Yihui Yuan[1,a,*]

[1]*Tibet University, Hebalin Campus, No. 36 Jiangsu Road, Jiri Street, Chengguan District, Lhasa City, Tibet Autonomous Region, China*
a. 2418539191@qq.com
**corresponding author*

Abstract: With the proliferation of network technology, cybercrime has become frequent, posing significant challenges to traditional legal theories and judicial practices. In response to the alienation of aiding behaviors in cyberspace compared to traditional legal acts, China introduced the offense of aiding information network criminal activities in 2015.Since its inception, the offense of aiding information network criminal activities has witnessed a transition from low to high application rates, accompanied by a surge in the number of related cases. As the pertinent legal framework has undergone continuous refinement, several issues have come to light, including disputes over the identification of assisted conduct and a tendency for the crime to become overly broad or catch-all offense in its scope. The improper expansion of judicial application poses a challenge to the principle of suitability of punishment to the crime committed. Thus, it is of great significance to study how to reasonably limit the application of this crime. Therefore, initiating a discussion on both legislative and judicial levels, grounded in the nature of this crime, its subjective patterns, and the punishable scope of neutral assisting behaviors, is crucial for addressing existing issues and refining legislation in the realm of cybersecurity in China. By reasonably distinguishing and analyzing issues such as "knowingly" and the punishability of neutral aiding behavior, we can effectively narrow the scope of this offense. Taking the restrictive interpretation as the fundamental stance, this article briefly analyzes the definition of the nature of the crime of aiding information network activities, the exploration of subjective and objective elements, and other restrictive approaches, aiming to benefit judicial practice.

Keywords: restrictive position, the offense of aiding information network criminal activities, cybercrime, the Leniency System for Those Who Confess and Plead Guilty

1. Introduction

The number of cybercrime cases is currently experiencing a rapid growth trend, with cybercrimes demonstrating characteristics of intelligence, complexity, and diversification. With the support of information network technology, the assistance behavior in cyberspace has undergone alienation. In response to the impact of cybercrime on traditional legislation and judicial practice, the Criminal Law Amendment (IX) in 2015 introduced the offense of assisting in information network criminal

DOI: 10.54254/2753-7048/2024.20818

activities during the legislative amendment process. The establishment of the the offense of aiding information network criminal activities is conducive to resolving the issue where traditional accomplice theories struggle to adapt to new situations and effectively combating cybercrime. However, with the official implementation of the crime and the progression of judicial practice, a series of problems have come to light. Debates on the nature of the offense of aiding information network criminal activities with illegal activities, such as whether it represents a sentencing rule that has not deviated from the traditional framework of accessory offenses, or whether it criminalizes helping behaviors as principal offenses in cyberspace, as well as issues such as whether neutral helping behaviors mentioned in legal provisions should be criminalized, have attracted widespread attention in academic circles. Zhang Mingkai believes that the establishment of the offense of aiding information network criminal activities cannot be separated from the existence of the principal offender and is a sentencing rule for specific accessory offenders. Li Hong supports the theory of sentencing rules and points out that this offense applies the relevant provisions on the punishment of accomplices in the General Principles of the Criminal Law. Furthermore, some scholars have pointed out that misjudgments in practice are one of the reasons for the large number of cases involving the offense of aiding information network criminal activities. Zhang Mingkai believes that due to misunderstandings of this crime, a large number of cases have been misjudged as the offense of aiding information network criminal activities in practice. Chen Hongbing believes that if the party subjectively has knowledge of this and the act objectively has causality with the online criminal acts and consequences committed by others, and if the act itself violates regulations, then in principle, the establishment of an accomplice to crimes such as fraud cannot be denied. The study on the reasonable legislation and application of the offense of aiding information network criminal activities must balance the modesty of criminal law while ensuring effective combating of cybercrime. Deviations are not dreadful; what is dreadful is the failure to promptly correct errors. This article attempts to clarify the application issues related to the offense of aiding information network criminal activities, with the aim of benefiting the application of this offense.

2. Existing Issues

With societal development and continuous advancements in network technology, traditional crimes such as gambling, pyramid schemes, and fraud have infiltrated cyberspace, posing severe hazards to society. The proliferation of information technology has further fueled a sharp increase in the number of cybercrime cases. The introduction of the offense of aiding information network criminal activities has catered to the need to combat information technology crimes. However, in the process of specific judicial practice, some issues have been exposed, prompting continuous reflection and exploration within the academic community.

2.1. The Nature of the Offense of Aiding Information Network Criminal Activities is Controversial

No matter what angle is taken to study the offense of aiding information network criminal activities, an exploration of its nature is indispensable. Due to the unique characteristics of cyberspace, related criminal acts and acts of aiding and abetting such crimes have undergone alienation compared to traditional criminal acts. On the one hand, in this era where people generally possess a certain level of computer literacy, the threshold for committing cybercrime assistance is not only low, but also the investment costs incurred by the criminals often do not commensurate with the resultant damages. With the support of network information technology, minimal costs, basic network technologies, and non-professional implementers can all potentially exert tremendous impact. This may not only lead to an increase in aiding and abetting criminal behavior but also result in a surge in direct cybercrime

DOI: 10.54254/2753-7048/2024.20818

cases, where the accessory nature of aiding behavior undergoes mutation, exerting a catalyzing and intensifying effect on criminal conduct. On the other hand, due to the transcendence of the internet over time and space, cybercrime assistance often manifests in a "one-to-many" model, where there may not be a clear criminal intent communication among those involved in cybercrime, causing difficulties in the identification of joint crimes. Thus, the offense of aiding information network criminal activities is distinguished from other helping behaviors and established as an independent crime, in order to address the current situation of numerous, rapidly growing, and complex and special network crime cases. However, whether the nature of the offense of aiding information network criminal activities is the principalization of aiding offenses or a newly established sentencing rule has become an issue that cannot be ignored. This pertains to a series of issues, including whether the offense of aiding information network criminal activities violates the principle of suitability of punishment to crime, and whether it is in conflict with the theory of neutral helping behavior. Currently, there is no consensus among academics on this issue. Scholars such as Liu Xianquan and Liu Yanhong argue that the offense of aiding information network criminal activities is essentially the embodiment of helping behavior being treated as principal conduct, pointing out that it should be regarded as a legislative phenomenon of treating helping behavior as principal conduct, rather than merely a sentencing rule. [1] This is also the mainstream view in the current academic circle, namely, that the offense of aiding information network criminal activities essentially criminalizes the act of aiding and abetting cybercrime as a principal offense. Zhang Mingkai disagrees with the view of treating it as the principalization of helping behavior, arguing that the application of the offense of aiding information network criminal activities conforms to the principle of accessory nature of accomplice. He puts forward a particular viewpoint, namely, whether from a literal or substantive perspective, the offense of aiding information network criminal activities is merely a sentencing rule for specific accessory offenders. [2] Li Hong emphasized the accessory nature of the offense of aiding information network criminal activities, pointing out that according to the legal provisions, this crime cannot constitute an independent offense without the person being assisted. The distinction between a principal offender and an accomplice does not depend on whether there is an independent statutory penalty. the offense of aiding information network criminal activities sets a minimum sentence for the helping behavior stipulated in this legal provision, which does not affect the legal status of the provisions on accomplices in the General Provisions. [3] Wang Huawei believes that, in view of similar legislative forms at present, there is no clear criterion for distinguishing the above two types of disagreements in nature. Furthermore, sentencing rules usually do not exhibit typological characteristics in legal provisions, and judges have discretionary power over them in practice. He pointed out that this issue should be viewed from the dual perspectives of improving legislative technique and mitigating criminal penalties, and that there is no need for excessive inquiry as long as these two legislative objectives are met. [4]

2.2. The relevant defining standards urgently require further confirmation

According to Article 287(2) of the Criminal Law, the constituent elements of the offense of aiding information network criminal activities are providing technical, financial, promotional, or other forms of assistance to others in their criminal acts, while "knowingly" that the others are using information networks to commit crimes. It encompasses the subjective aspect of "knowingly" and the objective aspect of aiding behavior. A reasonable and clear definition standard can effectively prevent problems in judicial practice. The issue of "knowingly" on the subjective level and the punishability of neutral aiding behavior on the objective level, both being constituent elements of the offense of aiding information network criminal activities, play a pivotal role in actual judicial practice and require further discussion.

DOI: 10.54254/2753-7048/2024.20818

2.2.1. Analysis Model of Criminal Intent

The traditional analysis model of crime as a whole encompasses two key elements: intention and consequence. Cybercrimes often exhibit a "chain-like" structure, relying on the support of network technology to transcend temporal and spatial constraints, such that individuals without criminal intent communication may also constitute a complete chain of cybercrime. For instance, telecommunication network fraud can be divided into several stages such as preparing criminal tools, building online platforms, developing application software, conducting telephone fraud, and cashing out and transferring funds. This disrupts the separation between preparatory acts, perpetrating acts, and subsequent acts in traditional criminal composition, blurring the boundaries between them. The upstream and downstream crimes do not require simultaneity, nor do they necessitate collaboration between the perpetrator and the executor. If the traditional holistic crime analysis model is applied, it may lead to a dilemma where the legislative and judicial practices conflict with the original legislative intent of effectively combating cybercrime from its source, due to the possible lack of clear criminal intent communication between those who provide assistance for cybercrime activities and the perpetrators themselves. At the outcome level, the establishment of criminal intent primarily hinges on the hope for or indulgence towards the harmful consequences, whereas individuals engaging in aiding conduct, especially neutral aiding conduct, may not necessarily possess a clear cognition of the harmful consequences, nor necessarily hold a hopeful or indulgent attitude towards them. In the holistic crime analysis model, the conflict between "knowingly" stipulated in legal provisions and post-event evaluation items tends to lead to an undue restriction on the scope of application of the offense of aiding information network criminal activities.

2.2.2. Objective Constituent Elements

At present, the identification of behavioral types for the offense of aiding information network criminal activities is still unclear. A typical controversy is whether the objective acts stipulated in this crime constitute neutral helping behavior. If it is deemed as a neutral and helpful act, it may conflict with the theory that the nature of the offense of aiding information network criminal activities is the principalization of a helping act. Liu Yanhong regards the behavior of helping information network criminal activities as a typical neutral helping behavior, pointing out that it is necessary to distinguish between "knowingly facilitating" and "knowingly non-facilitating" helping behaviors. She further notes that from the current judicial perspective, the offense of aiding information network criminal activities has led to the improper incrimination of the latter. [5] Although Zhang Mingkai does not deny that the objective conduct stipulated in the constituent elements of the offense of aiding information network criminal activities, as prescribed in Article 287(2) of the Criminal Law, may encompass neutral helping behaviors, he disagrees with the view that they all constitute neutral helping behaviors, pointing out that "an interpretation can be made in the direction of restricting the scope of punishment for neutral helping behaviors." [2] Interpreting the punishability of the objective elements of the crime of assisting in information network crimes from a restrictive standpoint, and limiting the punishment of "knowingly non-facilitative" helping acts in specific practices can reasonably identify neutral helping behaviors, which is conducive to correcting issues arising in current practices, such as the tendency of the offense of aiding information network criminal activities to become a catch-all offense.

2.3. The catch-all offense tendency of the offense of aiding information network criminal activities and the trend of unbounded expansion in its application

In judicial practice, the offense of aiding information network criminal activities has shown a trend of becoming a catch-all offense, which is inextricably linked to legislation. From the perspective of

DOI: 10.54254/2753-7048/2024.20818

legislative language, the relevant objective elements in the legal provisions are business-oriented, tending to categorize various neutral online behaviors. Furthermore, the expression "and other technical support" indicates that the offense possesses the characteristics of a flexible clause. The unclear discussion on key issues such as the criteria for identifying objective behaviors has led to the tendency of the offense of aiding information network criminal activities to become a catch-all offense in judicial practice. Additionally, there are also problems of insufficient and inadequate judicial interpretations in this regard. For instance, relevant judicial interpretations[6] further elaborate on the "support" and "assistance" of objective elements as "providing specifically for illegal crimes" and "enabling others to evade supervision or circumvent investigations." However, issues such as how to determine "specifically" and the clearly defined qualification criteria for "supervision" and "investigation" still pose challenges in judicial practice and await further stipulations in judicial interpretations. Since the official implementation of the offense of aiding information network criminal activities, its application rate has been continuously increasing, especially after the launch of the "Crackdown on Illegal Sim Cards and Bank Accounts"(hereinafter referred to as "the operation to cut off cards" in the following text) campaign in 2020, showing a trend of unlimited expansion, with a substantial surge in the number of cases. In the case involving Jonh Doe's offense of aiding information network criminal activities, he was sentenced to a term of imprisonment of ten months with a probation period of one year and two months, and fined RMB 1,000 yuan, for knowingly selling his bank card and Alipay account to others who were engaged in network criminal activities. There are numerous instances similar to Jonh Doe, who have turned into criminals for the sake of petty gains. However, the sole reliance on penal sanctions as a regulatory measure has, to a certain extent, undermined the modesty principle of criminal law.

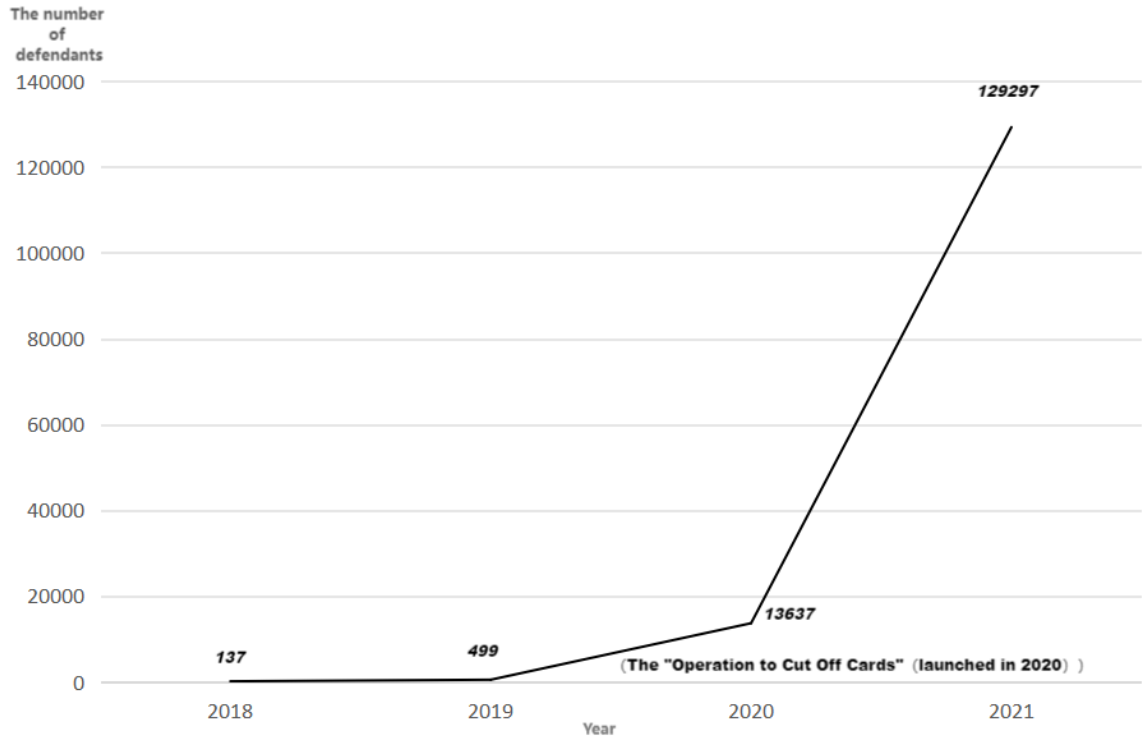

Figure 1: Line Chart of the Number of People Prosecuted for the offense of aiding information network criminal activities by the Procuratorial Organs Nationwide in China from 2018 to 2021.

DOI: 10.54254/2753-7048/2024.20818

3. Relief Pathway

Cybercrime is characterized by its complexity and specificity. In order to achieve the criminal legislative objectives of risk control and harm prevention, both legislation and judicature must adapt to the changing situation. In terms of legislation, while clarifying and improving relevant theories, it is necessary to adhere to a comprehensive consideration attitude and a restrictive interpretation stance, and to integrate theory with social reality on the basis of practical experience. In judicial practice, it is necessary to avoid both inadequate implementation and abuse as well as unlimited expansion. The principle of safeguarding human rights and freedoms must always be upheld, ensuring that the offense of aiding information network criminal activities does not become a fallback or catch-all offense that indulges judicial inertia and deviates from the principles of responsibility and suitability of punishment. Additionally, the introduction of Leniency System for Those Who Confess and Plead Guilty can be considered to conserve judicial resources. When discussing the relief path, it is imperative to grasp the core of the issue, namely, promoting a more reasonable application of the offense of aiding information network criminal activities. Currently, the improper expansion trend in the application of this crime is particularly prominent. Therefore, to discuss the dilemmas in the current application process, it is essential to adhere to the fundamental stance of restriction.

3.1. The clarification of nature

Some scholars argue that when exploring the nature of the offense of aiding information network criminal activities, it should be recognized that its fundamental purpose is to improve legislation and mitigate criminal law. To harmonize the application of the offense of aiding information network criminal activities with the provisions on joint crimes in the General Provisions of the Criminal Law, it is necessary to fully consider both subjective and objective factors in judicial practice, achieving a unity between the purpose of establishing this crime and the principles of safeguarding human rights and the suitability of punishment for the crime. When discussing the nature of the offense of aiding information network crime activities, the impact of legislative techniques on judicial practice should be comprehensively considered. This article argues that the offense of aiding information network crime activities represents an exploration of the theory of unilateral accomplice and should not be regarded solely as an indication of the principalization of aiding behavior. From the perspective of the causal complicity theory, distinguishing between a principal offender and an accomplice requires attention to the way in which an act causes legal interest damage. From the formulation of legal provisions, the offense of aiding information network criminal activities has not breached the subordinate nature of an accomplice. It primarily aids and abets in the harmful consequences rather than directly causing them, thus it is difficult to directly regard it as the principalization of helping behavior. From the perspective of the theory of unilateral joint offense, as long as the actor can or should recognize the criminal intent and criminal act of the person being assisted, the establishment of the accessory offense can be acknowledged. Exploring the nature of the offense of aiding information network criminal activities from the angle of unilateral joint offense is conducive to maintaining network security while exploring a judicial approach that combines leniency with severity with appropriate restrictions. Regarding the punishability of neutral helping acts, there are mainly two scholarly positions: the comprehensive affirmation theory and the restriction theory. Zhang Mingkai pointed out that "we can interpret in the direction of restricting the scope of punishment for neutral helping acts." Liu Yanhong argues that helping activities in cybercrime can be regarded as typical neutral helping behaviors. When assessing the types of objective behaviors, she proposes categorizing helping behaviors into two major types: "knowingly facilitating" and "knowingly non-facilitating," with the latter not constituting a criminal offense. Limiting the scope of punishable neutrality assistance behaviors is conducive to correcting the trend of over-

DOI: 10.54254/2753-7048/2024.20818

generalization of the offense of aiding information network criminal activities and preventing its unbounded expansion in judicial practice.

3.2. Selection of Analytical Modes for Criminal Intent

The complexity, sophisticated division of labor, and difficulty in obtaining evidence in cybercrime cases mean that not only can helping behaviors be independent of perpetrating behaviors, but the subjective intent of those providing assistance in information networks may also be separate from the direct perpetrators of cybercrimes. From the perspective of current judicial practice cases, the characterization of such cases places significant emphasis on whether the perpetrator had knowledge or not.

Table 1: Four typical cases where the judgment outcome is influenced by whether the perpetrator had knowledge.

Name of the Case	verdict
Case of Yang Xhua aiding information network criminal activities	The defendant Yang XH had a single-thread connection with the upstream personnel. Since he had obtained benefits from providing fund accounts to the upstream in the early stage and **had a general awareness** of the upstream's cybercrime activities, and later rented a house to set up a specialized fund transfer site to provide payment and settlement assistance to the upstream, his conduct still fell within the scope of the crime of assisting in information network crimes. Therefore, he was convicted and punished for the offense of aiding information network criminal activities.
Case of Ma XX and Mao XX aiding information network criminal activities	The perpetrator of this case **knew** that others were using information networks to commit crimes and provided technical support through GOIP equipment, which constitutes a serious circumstance. Therefore, convicting and punishing the perpetrator for the offense of aiding information network criminal activities is consistent with the principle of suitability of punishment for the crime.
Case of Long XX involving the offense of aiding information network criminal activities	After review and remanding for supplementary investigation by the court, it was still deemed that the criminal facts identified by the Huachi County Public Security Bureau were unclear and the evidence was insufficient. The actions carried out by the non-prosecuted person, Long XX, played only an auxiliary role. The current evidence is limited to inconsistent verbal statements, lacking objective evidence. **There is insufficient evidence to determine whether Long XX knowingly** used Liu XX's Alipay

DOI: 10.54254/2753-7048/2024.20818

Table 1: (continued).

	account to transfer criminal funds or whether he knowingly assisted the individuals he transported in providing help to the criminal syndicate.
Case of Zhang XX involving the offense of aiding information network criminal activities	Zhang XX has made a total of three interrogation records regarding the facts of the case at the public security organ, and only in the first record did he state that he took a lax attitude towards the illegal and criminal activities conducted by accounts registered through the code receiving platform using the verification codes he sent; Chen XX has made a total of five interrogation records regarding the facts of the case at the public security organ, and none of them contained any confession regarding subjective knowledge of the offense. During the court review, both individuals stated that **they did not know** that the accounts registered through the verification codes they sent would be used by criminals to conduct illegal information network activities, and the code receiving platform assured them that it would not be used for illegal purposes. Currently, the personnel involved with the "Shang Yipin" code receiving platform have been sentenced, but the judgment did not involve the two criminal suspects in this case. Therefore, regarding the subjective knowledge or ought-to-know status of the two individuals concerning the illegal information network activities conducted by accounts registered through the code receiving platform using the verification codes they sent, Zhang XX's confessions are contradictory, Chen XX has made no confession related to guilt, and there is no other evidence to support this. It is unclear and insufficiently evidenced to determine that Zhang XX constitutes the offense of aiding information network criminal activities, **which does not meet the prosecution conditions.**

The traditional analysis model of criminal intention struggles to address the alienation of criminal intention in cyberspace. In order to effectively combat cybercrime, it is an inevitable choice to lower the standards for determining certain objective constituent elements. Based on the characteristics of China's criminal constituent system, Zhang Mingkai conducted a comparative study of German and Japanese criminal law. Drawing on the views of scholars such as Birmingham and Naito Ken, who

DOI: 10.54254/2753-7048/2024.20818

regard objective punishment conditions as constituent elements, he summarized the insights brought by the concept of "subjective super-elements" and created the concept of "objective super-elements" to address the identification dilemma where the perpetrator intentionally commits a crime but does not intentionally cause the resulting consequences. The theory of "objective super-elements" examines the result-oriented stance of the traditional analysis model of intentional crimes and points out that in determining the intention of the offense of aiding information network criminal activities, it is not necessary to require the perpetrator to have a hopeful or indulgent attitude, and even the requirement for the perpetrator to have knowledge may be dispensed with. However, there is still room for improvement in this theory. Lao Dongyan points out that the application of the " objective super-elements " theory tends to promote an abstract understanding of harmful consequences, leading to double standards in determining the establishment of intention. In response, scholars such as Lao Dongyan and Huang Mingru suggest that adopting the element analysis model may be a viable approach to address this issue. The element analysis model acknowledges that different objective factors within the same intentional offense may necessitate the application of distinct forms of culpability, meaning that while an intentional act is required for the behavioral element, negligence may suffice for the consequential or other circumstantial elements. The surge in the number of cybercrime cases and the escalating complexity of these cases have led to a mismatch between the traditional theory of criminal intent and societal demands for risk control. Compared to the traditional analysis model of criminal intent, the element analysis model is better suited to meet the practical needs of risk control and harm prevention. Furthermore, it is crucial to guard against a shift in research focus. Chen Hongbing points out that grasping the three elements of "illegality," "principal offender," and "causality" is the key to properly addressing issues related to aiding behavior. [7] Regardless of the analytical model chosen, the core should always be to benefit justice.Assessing the Feasibility of Introducing the Leniency System for Those Who Confess and Plead Guilty into the Criminal Litigation Process

In addressing the rising number of cases involving the offense of aiding information network criminal activities, we can explore the feasibility of applying the Leniency System for Those Who Confess and Plead Guilty in the process of handling such crimes, in order to alleviate the pressure on the judicial system. Since its official application, the conviction rate for the offense of aiding information network criminal activities has been increasing. The Leniency System for Those Who Confess and Plead Guilty facilitates the simplification of criminal proceedings and alleviates the burden on judicial authorities. If criminal suspects voluntarily confess to their crimes, truthfully admit their guilt, and accept the sentencing recommendations of the procuratorial authorities, they can generally strive for leniency in sentencing. The rational and appropriate application of the Leniency System for Those Who Confess and Plead Guilty not only facilitates the achievement of the legislative purpose of mitigating criminal penalties but also conserves judicial resources. However, the following issues also need to be considered. Firstly, the sentencing standards for the offense of aiding information network criminal activities are relatively low, with a maximum imprisonment of not more than three years or criminal detention, and a fine shall be imposed concurrently or independently. If the Leniency System for Those Who Confess and Plead Guilty is applied, the verdict may fail to deter crimes effectively. Secondly, the Leniency System for Those Who Confess and Plead Guilty requires suspects to voluntarily and truthfully confess their criminal facts. However, in cases involving the offense of aiding information network criminal activities, the perpetrators of helping behaviors may not have a clear understanding of the upstream criminal facts. If they are only required to confess their own helping behaviors, it would violate the theory of accessory liability in criminal law. Thirdly, the Leniency System for Those Who Confess and Plead Guilty itself needs to be improved. In practice, there are cases where defendants are convicted due to their guilty plea despite doubts surrounding the conviction. The application of the Leniency System for Those Who Confess and Plead Guilty in the

DOI: 10.54254/2753-7048/2024.20818

offense of aiding information network criminal activities has certain feasibility, but its effectiveness is influenced by various practical factors, including the specific circumstances of the case, local policies, and judicial discretion of judges.

4. Conclusion

The cyberspace is characterized by weak territoriality and complexity. With the support of information and network technology, some traditional crimes undergo alienation in cyberspace. In order to better prevent and govern cybercrime issues, the law must evolve in accordance with the situation. The introduction of the offense of aiding information network criminal activities catered to the need to combat the chain of cybercrime. However, the application of this offense still faces some issues, such as the trend of improper expansion. This expansion not only tends to turn the offense into a catch-all offense but also easily leads to deviations from the fundamental principles of criminal law. Therefore, adjusting the offense of aiding information network criminal activities from the perspective of restriction is not only a necessary correction to the existing problems but also an adherence to the principle of restraint in criminal law. In judicial practice, the boundaries and objects of objective helping behaviors related to the offense of aiding information network criminal activities have shown an expanding trend. To this end, it is imperative to clarify the nature of this crime and prevent "knowingly non-facilitating" neutral helping behaviors from being improperly criminalized. Furthermore, regarding the issue of judicial over-application in the context of the offense of aiding information network criminal activities, it is advisable to explore the feasibility of introducing the Leniency System for Those Who Confess and Plead Guilty and appropriately broaden the scope of discretionary non-prosecution. This not only helps reduce unnecessary consumption of judicial resources but also facilitates the swift handling of cases and the realization of legal effects. In summary, by exploring the nature of this offense, subjective patterns, the punishable scope of neutral and accessory acts, and other issues, and adhering to a restrictive stance in both legislative and judicial aspects, we can effectively curb its tendency of improper expansion and ensure the implementation of the principle of modesty in criminal law. This will not only help maintain the solemnity and authority of the law but also better meet the practical needs of combating cybercrime. In judicial practice, it is imperative to adhere to the substantive restriction of the offense of aiding information network criminal activities, in order to achieve effective application of criminal law and maintain stable social order. While clarifying and refining relevant theories, it is essential to adhere to a comprehensive consideration attitude and a restrictive interpretation stance. Only by consistently upholding the principle of safeguarding human rights and applying both leniency and severity appropriately can we prevent the offense of aiding information network criminal activities from becoming a catch-all offense that indulges judicial inertia and deviates from the principles of responsibility and the suitability of punishment to the crime.

References

[1] *Liu Xianquan, Fang Huiying. Difficulties in Identifying the Offense of Aiding Information Network Criminal Activities [J]. People's Procuratorate, 2017(19): 9-12.*

[2] *Zhang Mingkai. On the Offense of Aiding Information Network Criminal Activities [J]. Politics and Law, 2016, (02): 2-16. DOI: 10.15984/j.cnki.1005-9512.2016.02.001.*

[3] *Li Hong. On the Nature and Application of the Offense of Aiding Information Network Criminal Activities [J]. Law Application, 2017, (21): 33-39.*

[4] *Wang Huawei. A Critical Interpretation of the Principalization of Helping Acts in the Online Context [J]. Law Reviews, 2019, 37(04): 129-138. DOI: 10.13415/j.cnki.fxpl.2019.04.011.*

[5] *Liu Yanhong. A Critique on the Principalization of Assistance in Cybercrime [J]. Studies in Law and Business, 2016, 33(03): 18-22. DOI: 10.16390/j.cnki.issn1672-0393.2016.03.004.*

DOI: 10.54254/2753-7048/2024.20818

[6] *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Networks and Assisting in Information Network Criminal Activities [N]. People's Procuratorate Daily, 2019-10-26(003).*

[7] *Chen Hongbing. Correcting the "Catch-all Offense" Tendency of the Offense of Aiding Information Network Criminal Activities [J]. Journal of Hunan University (Social Science Edition), 2022, 36(02): 127-135. DOI: 10.16339/j.cnki.hdxbskb.2022.02.017.*